

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): KIMURA, Junichi  
Serial No.: Not yet assigned  
Filed: June 25, 2003  
Title: SCRAMBLER, DESCRAMBLER AND THE PROGRAM FOR  
SCRAMBLING OR DESCRAMBLING  
Group: Not yet assigned

LETTER CLAIMING RIGHT OF PRIORITY

Honorable Commissioner of  
Patents and Trademarks  
Washington, D.C. 20231

June 25, 2003

Sir:

Under the provisions of 35 USC 119 and 37 CFR 1.55, the applicant(s)  
hereby claim(s) the right of priority based on Japanese Patent Application No.(s)  
2002-305288, filed October 21, 2002.

A certified copy of said Japanese Application is attached.

Respectfully submitted,

ANTONELLI, TERRY, STOUT & KRAUS, LLP



---

Carl I. Brundidge  
Registration No. 29,621

CIB/alb  
Attachment  
(703) 312-6600

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2002年10月21日

出 願 番 号

Application Number:

特願2002-305288

[ST.10/C]:

[JP2002-305288]

出 願 人

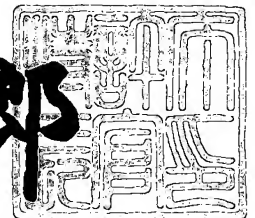
Applicant(s):

株式会社日立製作所

2003年 5月23日

特 許 庁 長 官  
Commissioner,  
Japan Patent Office

太田信一郎



出証番号 出証特2003-3038536

【書類名】 特許願

【整理番号】 H02013981A

【あて先】 特許庁長官 殿

【国際特許分類】 H04L 9/20

【発明者】

【住所又は居所】 東京都国分寺市東恋ヶ窪一丁目 2 8 0 番地 株式会社日立製作所中央研究所内

【氏名】 木村 淳一

【特許出願人】

【識別番号】 000005108

【氏名又は名称】 株式会社 日立製作所

【代理人】

【識別番号】 100075096

【弁理士】

【氏名又は名称】 作田 康夫

【電話番号】 03-3212-1111

【手数料の表示】

【予納台帳番号】 013088

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 デジタル映像スクランブル装置、デスクランブル装置および該装置を実現するプログラム

【特許請求の範囲】

【請求項 1】

デジタル符号化された入力映像ストリームの内容を解析しヘッダ部分を検出する手段と、

乱数を発生させる手段と、

上記乱数を用いて上記検出されたヘッダ部分以外を入力映像ストリームの換字位置を決定する手段と、

上記決定された位置の換字処理を行うスクランブル手段と、

上記スクランブル処理された映像ストリームを出力する手段と、を有することを特徴とするデジタル映像スクランブル装置。

【請求項 2】

上記入力映像ストリームに対応するスクランブルレベルを指定する情報を入力する手段と、

秘密鍵を生成する手段と、

上記入力された情報を上記秘密鍵を用いて暗号化して出力する手段とを更に有し、

上記換字位置決定手段は、上記乱数に加えて上記情報を用いることを特徴とする請求項 1 記載の映像スクランブル装置。

【請求項 3】

乱数を発生させて、上記換字表を作成する手段をさらに有し、

上記スクランブル手段は、上記換字表を用いて上記換字処理を行うことを特徴とする請求項 1 又は 2 に記載のスクランブル装置。

【請求項 4】

上記スクランブル手段を複数有し、

上記複数のスクランブル手段それぞれに対応する換字位置を決定する手段と、

上記換字位置を上記複数のスクランブル手段に割り当てる手段とを有することを

特徴とする請求項 1 乃至 3 の何れかに記載のスクランブル装置。

【請求項 5】

請求項 1 記載のスクランブル装置にネットワークを介して接続されるデスクランブル装置であって、上記換字処理された入力映像ストリームを取得する手段と、上記入力映像ストリームの内容を解析しヘッダ部分を検出する手段と、秘密鍵をもとに乱数を発生させる手段と、上記乱数を用いて上記ヘッダ部分以外の換字復元位置を決定する手段と、上記決定された位置の換字復元処理を行う手段と、を有することを特徴とするデジタル映像デスクランブル装置。

【請求項 6】

上記ネットワークを介して識別情報を出力する手段と、上記識別情報に基づいた認証の結果送出された上記秘密鍵を、上記ネットワークを介して受信する手段と、を有することを特徴とする請求項 5 記載のデジタル映像デスクランブル装置。

【請求項 7】

乱数を発生させて換字テーブルを作成し、記録手段に記録するステップと、上記換字テーブルをネットワークを介して出力するステップと、入力手段を介して映像信号を取得するステップと、上記映像信号の信号を読み込み、該信号の符号化の構文を解析するステップと、該信号についての換字を行うか決定するステップと、上記換字を行うと判定された場合には、該信号を上記換字テーブルに従って変換するステップとを有し、上記信号に続く信号を読み込み上記ステップを上記映像信号がなくなるまで繰り返し、上記換字を行うかの決定基準は上記解析結果に応じて変更することを特徴とする符号化プログラム。

【請求項 8】

上記換字テーブルは暗号化して出力され、該暗号化解除に必要な鍵情報を上記符号化された信号の出力先のコンピュータと交換するステップをさらに有することを特徴とする請求項 7 記載の符号化プログラム。

ラム。

【請求項 9】

符号化された信号と暗号解読の情報と該符号化に用いた換字テーブルの情報をネットワークを介して取得するステップと、  
 該換字テーブルの情報から対応する逆換字テーブルを作成し、記憶手段に記憶するステップと、  
 該信号を読み込み該信号の符号化の構文を解析するステップと、  
 上記解析結果を用いて上記信号を逆換字するか判断するステップと、  
 上記逆換字すると判断された信号を上記逆換字テーブルを用いて逆換字するステップと、  
 上記読み込んだ信号の次の信号を読み込んで上記ステップを繰り返すことを特徴とする復号化プログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は映像配信システムに係わり、デジタル符号化した映像の一部が視聴可能なスクランブル方法に関する。

【0002】

【従来の技術】

映像をデジタル的に符号化（圧縮）する方法は、非特許文献 1 にて定められている。これらの符号をサーバから端末に配信する場合、限られた端末にのみ限定的に映像を配信する第 1 の方法として、データの暗号化がある（例えば、非特許文献 2 参照）。しかし、データの暗号化を用いると、暗号鍵を持っている端末は視聴可能だが、暗号鍵を持っていない端末では、データの内容は完全に攪拌されてしまうため、映像の一部を試みに視聴することは全くできない。

第 2 の方法としては、スクランブル機能のある映像符号化（スクランブル機能付き映像符号化）が知られている（例えば、特許文献 1 参照）。スクランブル機能付き映像符号化では、符号化時に符号化するデータの内容を僅かに変動させるため、鍵を持っていない端末においても部分的に視聴することが可能となる（一部

意図的に劣化した画像の視聴も含む。以下部分視聴と表現する）。部分視聴ができると、暗号鍵を持っていない端末でも、映像コンテンツの様子・概要等を視聴することができるため、暗号鍵の購入等を促進する効果が高く、優良な映像配信、特に映像の同報配信においては有効な手段である。

なお、以下、スクランブルと暗号化は同義とする。

【特許文献 1】

特開平 1 0 - 1 4 5 7 7 2 号公報

【非特許文献 1】

アイ エス オー／アイ イー シー ISO/IEC 14496-2 (MPEG-4)、アイ エス オー／アイ イー シー ISO/IEC 13818-2 (MPEG-2)

【非特許文献 2】

PKCS #1: RSA Cryptography Specifications Version 2.1, An RSA Laboratories Technical Note

【 0 0 0 3】

【発明が解決しようとする課題】

上記の従来技術において、暗号化においては、映像コンテンツの部分視聴ができない。また、スクランブル機能付き映像符号化では、映像コンテンツを符号化する時に、スクランブルの有無あるいは強度等を設定する必要があるため、配信中継者がスクランブルをかけたり、符号化時と異なる強度のスクランブルをかけることができず、利便性を著しく欠いている。

本発明は、デジタル符号化されたコンテンツに対し、利便性を有する部分視聴可能なスクランブル方法を提供することを目的とする。

【 0 0 0 4】

【課題を解決するための手段】

上記目的を達成するために、符号化された映像コンテンツの画像データ部分の一部を暗号化することにより実現する。本願の開示する発明の代表的なものを示せば以下の通りである。デジタル符号化された入力映像ストリームの内容を解析しヘッダ部分を検出し、発生した乱数を用いて上記検出されたヘッダ部分以外を入力映像ストリームの換字位置を決定し、決定された位置の換字処理を行うス

クランブル手段を有するデジタル映像スクランブル装置。

【 0 0 0 5 】

【発明の実施の形態】

以下本発明による第 1 の実施例を図 1 に示す。図 1 は、映像配信側 1 0 1 および、映像受信側 1 0 2 から構成され、配信側の中のスクランブラ 1 0 0、デスクランブラ 1 0 3 の部分が本発明において特徴ある個所である。

【 0 0 0 6 】

以下、動作の概要を説明する。映像配信開始に先立ち、暗号鍵生成部 1 3 0 にて暗号鍵 1 3 1 が、パラメータ生成部 1 2 0 にてスクランブルパラメータ 1 2 1 が生成される。暗号鍵 1 3 1 は、配信するコンテンツを正しく符号化し視聴するための鍵である。また、スクランブルパラメータはスクランブルを実行する上で、送信・受信双方にて共有するパラメータであり、後述する。

映像配信の指示があると、まず、送信暗号鍵交換部 1 3 2 と受信鍵交換部 1 3 4 の間にて、暗号下記の送信が行われる。一般に、暗号鍵交換は PKCS #3: Diffie-Hellman Key-Agreement Standard、An RSA Laboratories Technical Note に開示されている方法等の秘匿性の高い方法により行われるが、鍵交換の方法選択は本発明とは独立の問題であり、本発明ではいかなる鍵交換法あるいは、秘匿性を持たない鍵交換（暗号化しない鍵配送）とも組み合わせが可能である。

【 0 0 0 7 】

鍵交換が完了し、受信側にて受信暗号鍵 1 3 5（暗号鍵 1 3 1 に対応）を取得すると、次にスクランブルパラメータの伝送が行われる。スクランブルパラメータ 1 2 1 は、暗号部 1 2 2 において、暗号鍵 1 3 1 を用いて暗号化され、秘匿スクランブルデータ 1 2 3 として配信される。受信側では、受信した秘匿スクランブルデータ 1 2 3 を先の受信暗号鍵 1 3 5 を用いて、暗号解読部 1 2 4 において解読され、スクランブルパラメータ 1 2 1 に対応する受信スクランブルパラメータ 1 2 5 が得られる。

【 0 0 0 8 】

スクランブルパラメータを送信・受信にて共有した後、映像の配信が行われる。すなわち、映像ストリーム 1 1 1 はスクランブル部 1 1 2 にて、スクランブル



パラメータ 1 2 1 を用いて、そのデータの一部が変換されスクランブルストリーム 1 1 3 として出力される。一方受信側では、スクランブルストリーム 1 1 3 を受信し、デスクランブル部 1 1 4 において、受信スクランブルパラメータ 1 2 5 を用いてスクランブルの解除を行い、解除したストリーム 1 1 5 (映像ストリーム 1 1 1 と同一) を再生部 1 1 6 に送り、再生画像 1 1 7 を得る。

## 【 0 0 0 9 】

図 2 から図 5 を用いて、スクランブル部 1 1 2 の詳細な構成を示す。

入力される映像ストリーム 1 1 1 は、例えば、MPEG-2 や MPEG-4 においては、ヘッダ部とデータ部に分けられる。ヘッダ部はヘッダに引き続くデータを復号する上で必要なパラメータ (例えば、画像サイズや、画像の時間的位置等) を格納しており、ヘッダを識別するために、ヘッダ部の先頭はヘッダ以外では出現しないスタートコード (例えばビット " 0 " が 2 3 個連続し、次にビット " 1 " が出現する、これを 8 ビット毎に上位ビットから並べ 1 6 進数表示すると 0 x 0 0、0 x 0 0、0 x 0 1 となる。" 0 x " は以降が 1 6 進数であることを示す) が使用される。

## 【 0 0 1 0 】

データ部では、映像データ自体のデータが格納されており、一般に可変長符号により符号化されている。可変長符号は、例えばデータ A の符号は " 1 "、B は " 0 1 "、C は " 0 0 1 0 0 "、D は " 0 0 1 0 1 "、E は " 0 0 1 1 0 "、F は " 0 0 1 1 1 " のように、シンボルと 2 進のビット列が 1 対 1 に対応する。上記の例では、入力データが " 1 0 0 1 0 1 0 1 0 1 0 0 1 1 0 1 1 0 1 " の時は先頭からデータを調べて行き、" 1 [A] 0 0 1 0 1 [D] 0 1 [B] 0 1 [B] 0 0 1 1 0 [E] 1 [A] 1 [A] 0 1 [B] " のように区切り、出力シンボル A D B B E A A B を得る。得られたシンボルの意味およびこれらから映像の再生方法は、全て MPEG-2 あるいは MPEG-4 の規格にて規定されている。データ部では先のヘッダ部のスタートコードが絶対に出現しないように設計されている。例えば、上記シンボル A ~ F の例では、どのようなシンボルの組み合わせを行っても " 0 " は 5 つ以上連続しない。また、データ部では、可変長符号の特性上、1 ビットでもデータが欠落・反転するとそれ以降のデータが正しく再生できない。上記

入力データ例において、3ビット目が反転して”1”になると、”1 [A] 0 1 [B] 1 [A] 0 1 [B] 0 1 [B] 0 1 [B] 0 0 1 1 0 [E] 1 [A] 1 [A] 0 1 [B]”となり、出力シンボルA B A B B B E A A Bが得られ、正しい場合のシンボルA D B B E A A Bとデータが異なる上、シンボル数自体が8個から10個に変わってしまう。さらに、MPEG-2あるいはMPEG-4では、1つのシンボルの内容により、次のデータのタイプ、符号テーブルが異なることが多く、データ欠落・反転後の再生を困難にしている。

#### 【0 0 1 1】

スクランブル部112では、入力された映像ストリームのヘッダ部分を保護し、非ヘッダ部分、すなわちデータ部分（の一部）のみに対して換字処理201によりスクランブルをかけることにより、鍵を持たない端末における部分視聴の画質の適切な制御を行う。入力データを8ビット毎にまとめて16進数表示するとすると、ヘッダ部のスタートコードは0x00、0x00、0x01となるため、図2のデータ解析部202にて、8ビットのデータが入力される毎に、スタートコードを認識し、最後の0x01が入力された時点でスタートコード信号203を「検出」を示す状態にする。また、同時に、スタートコード直後のデータにより、そのヘッダの種類をヘッダタイプ206として出力する。さらに、ヘッダタイプが、フレーム（画面）のヘッダ（pictureヘッダあるいはVOPヘッダ）の場合は、該当フレームの符号化タイプ（単独で復号可能なイントラ-VOPあるいはI（イントラ）ピクチャ、前フレームからの差分信号により構成されるP-VOPあるいはPピクチャ、他のフレームの予測には使用しないB-VOPあるいはBピクチャ）を符号化タイプ207としてその種別を出力する。

#### 【0 0 1 2】

制御部204では、入力信号111の8ビット毎のタイミングにおいて、スタートコード信号203、ヘッダタイプ206、符号化タイプ207を解析し、該当する入力信号の8ビットデータに対してスクランブルをかけるか否かを決定する。スクランブルをかける場合には、入力された8ビットを後述する換字表に従い、所定の8ビットデータに変換し出力する。このデータの変換により、鍵を持たない受信側では、データの解読が正しく行われず、再生画像が劣化する。

## 【 0 0 1 3 】

図 3 に制御部 2 0 4 におけるスクランブル可否を決定するための状態遷移図を示す。スタートコードが検出されるといずれの状態においても、状態 3 0 4 に遷移する。これ以降しばらくの間はスクランブルは行わず、ヘッダ情報をそのまま出力する。具体的には、状態 3 0 4 において、次データが入力されると、状態 3 0 5 に遷移し、所定バイト数（M バイト）の間、換字指示信号 2 0 5 を OFF にしてスクランブルを抑制する。ここで M の値は、ヘッダタイプ 2 0 6 あるいは、フレームタイプ 2 0 7 により決定される。例えば、M の値は各ヘッダの標準的な長さよりも大きくし、かつ、フレームタイプが I-VOP あるいは I ピクチャの時は一般的に 1 フレームのデータ量が多いため M は大きめに、P-VOP あるいは P ピクチャの時は M の値はやや小さく、B-VOP あるいは B-picture の場合にはさらに短くする。

## 【 0 0 1 4 】

M バイトのデータの処理が終了すると、状態 3 0 5 から状態 3 0 1 に遷移し、その時点でのスタートコードの状態により状態 3 0 2 あるいは状態 3 0 4 に遷移する。状態 3 0 1 においては、データ部を処理する状態 3 0 2、3 0 3 におけるパラメータ N を定める。N は状態 3 0 2 において、換字を実行するまでのバイト数を表す。N バイトのデータを入力、すなわち換字を行わずに伝送することを終了すると、状態 3 0 3 に遷移し、換字指示信号 2 0 5 が ON になり、次の 1 バイトが換字される。N の値が小さいと、先に説明した画像の劣化が頻繁に起こり、N の値が大きいと、画像の劣化は少なくなる。例えば、N の値は次の式により生成する。

$$N = A + B * RND(C)$$

ここで、A、B、C はスクランブルパラメータとして、予め、フレームタイプ毎に設定され、RND(C) は 0 以上 C 未満の乱数であり、N の値を計算する毎に、予め定められた計算方法により生成される。この乱数の初期値はスクランブルパラメータとして受信側に伝送されるため、送信・受信双方にて乱数値は一致しており、受信側では、送信側において換字を行ったデータ位置を知ることができる。乱数の生成方法は、電子情報通信学会技術研究報告、ISEC2001-8、2001 等任意の方法を使用することができる。尚、本願で用いる乱数の語には疑似乱数も含

むものとする。

【 0 0 1 5 】

A, B のパラメータの大きさは部分視聴の画質に影響するため外部より直接的あるいは間接的に指定するが、このとき、ストリームの内容を反映させると、より部分視聴時の画質を所望の画質（劣化）に近づけることができる。具体的には、I/P/BのピクチャのタイプごとにA, Bのセットを切り替える。特に、軽い（劣化の少ない）部分視聴を実現するためには、PピクチャのA, Bの値を大きくすることにより、予測画像が劣化することによる、劣化の蓄積を抑えることができ安定した画質になる。

【 0 0 1 6 】

さらに、A, Bのパラメータを決定する時に、入力ストリームの全部あるいは先頭部分等の一部を事前に検査したり、スクランブルをかけながらストリームの特性を測定することにより、パラメータの修正を行い、より所望の部分視聴画質に近づけることが可能となる。具体的にはイントラピクチャ（VOP）の挿入頻度、イントラマクロブロックの挿入頻度、ビデオパケットのデータ長、スライスあるいはGOBのデータ長等の1つあるいはこれらの組み合わせを測定する。これらの値は、データエラーに対する耐性に影響する。例えば、イントラピクチャが頻繁に挿入されているときは、エラーから回復しやすくなる。これらの測定値をビットレート、フレームレート、画像サイズから導き出される、あるいは予め定められた所定の範囲と比較し、範囲外の時はエラー耐性の強弱に応じてスクランブルパラメータを変更する。

【 0 0 1 7 】

また、たとえば、3段階のレベル（1～3）の部分視聴の画質を想定し、レベルが3のときはIピクチャは部分視聴、P,BピクチャはA, Bを極端に小さくして部分視聴をほとんど不可にし（完全スクランブル）、レベルが2の時はIピクチャはスクランブルなし、P,Bピクチャは完全スクランブル、レベルが1の時はI,Pピクチャはスクランブルなし、Bピクチャは完全スクランブルとすることにより、他段階レベルの部分視聴映像を実現できる。

図4は、以上の処理を、ソフトウェアにて実装した場合のフローチャートである

。送信側の初期化 4 0 5、受信側の初期化 4 5 5 までは、前述の処理と同じである。ここで、換字テーブル(表) 生成 4 0 0 および、逆換字テーブル生成 4 5 0 については、図 5、6 を用いて後述する。

#### 【 0 0 1 8 】

初期化が終了すると、送信側においては入力ストリームを 1 バイト入力し、構文解析 4 1 0、図 3 の状態遷移に従った方法にてスタートコードの解析を行う。換字判定 4 1 5 では図 3 の状態に応じた換字指示信号 2 0 5 に該当する値により次のデータに対して換字処理を施すか否かを決定し、換字処理を実行する場合には 4 2 0 において換字を行い、換字を行ったあるいは行っていないデータを出力する。受信側においては、入力されたデータ、すなわち送信側が処理して出力したデータを入力し、上記の送信側とまったく同じ動作を行う。ただし、換字逆変換処理 4 7 0 においては、送信側の換字を元にもどす、逆変換処理を行う。

#### 【 0 0 1 9 】

図 5 は換字表の例である。列 5 0 0 は 8 ビットの入力データ (2 5 6 種類) であり、列 5 0 1 は列 5 0 0 の各データに対する出力値である。ここで、入力データ " 0 0 0 0 0 0 0 0 " (列 5 0 2) と入力データ " 0 0 0 0 0 0 0 1 " (列 5 0 3) は、入力と出力が常に同一である。この 2 つのデータの入出力を同一にすることにより、スタートコードを完全に保存することができる。残りの行 (行 5 0 4) は入力値 0 x 0 2 から 0 x F F の範囲の値がランダムに並べられており、それぞれの出力は重複しない。すなわち、出力値が a となる入力値 b は一意に定まる。

#### 【 0 0 2 0 】

図 5 の換字表はスクランブルパラメータとして送信・受信双方にて共有される。受信側では、図 5 の出力列 5 0 1 を入力、入力列 5 0 2 を出力とした表を用いることにより、送信側において換字を行ったデータを正しいデータに復元できる。

図 5 の換字表は、固定の表を用いてもよいし、複数コンテンツ毎、コンテンツ毎あるいは、コンテンツの部分毎 (例えば、所定フレーム数毎等) に、新規生成されてもかまわない。スクランブルされたデータの不正解読 (正規に鍵を得ない者

がスクランブルデータを解読すること)を防止するために、なるべく頻繁に換字表を交換し、かつ、換字表はその都度新規生成することが望ましい。

#### 【 0 0 2 1 】

図 6 に換字表生成アルゴリズムの例を示す。換字表は `tbl` との名の 2 5 6 の配列に格納され、 $i$  番目 ( $i = 0 \sim 255$ ) の出力データは `tbl[i]` として表現される。例えば、図 5 の表を表す場合 `tbl[0]=0`, `tbl[1]=1`, `tbl[2]=0xB4`, `tbl[3]=0x2A`,...である。

処理 6 0 1、6 0 2 において初期化を行う。すなわち、データ 0、1 に固定値をセットした後、残りのデータ (2 ~ 2 5 5) に - 1 をセットする。これ以降、配列の値が 0 以上 (2 5 5 以下) の場合は、既にその配列にはデータがセットされていることを示し、- 1 である場合はデータがセットされていないことを示す。

#### 【 0 0 2 2 】

初期化終了後処理 6 0 3 以降のループを 2 5 4 回処理を行う。ループ処理は 2 を初期値とする変数  $i$  によって行う。ループ内では、まず、処理 6 0 3 にて 0 ~ 2 5 5 までの範囲の乱数を発生させ ( $j$  に代入)、処理 6 0 4 にて `tbl[j]` にデータがセットされているか否かを確認する。セットされていない場合は、処理 6 0 5 に移り、`tbl[j]` に  $i$  を代入する (セットする)。既に `tbl[j]` がセットされている場合は処理 6 0 6 に移り、 $j$  を歩進 (2 5 5 を超えた場合は 2 にリセット) させて行き、セットされていない `tbl[j]` を検索する。その後、検索した時の  $j$  の値を用いて、処理 6 0 5 にて  $i$  をセットし、1 回のループ処理を完了する。この処理により、`tbl[]` の配列には 0 ~ 2 5 5 の値が重複せず入力される。

#### 【 0 0 2 3 】

また、別の生成例では、`tbl[i]=i` と初期化した後、2 から 2 5 5 の間の乱数を 2 つ ( $p$ ,  $q$ ) 発生させ `tbl[p]` と `tbl[q]` の値をそれぞれ交換する。この交換処理を十分な回数行くと、出力がランダムになる配列が生成できる。

上記いずれのアルゴリズムの場合でも、1 つの系列の乱数があれば、送信、受信双方にて同一の換字表を生成することができる。従って、スクランブルパラメータとしては 2 5 6 要素の換字表を設定・送信しても構わないし、乱数生成法を送受で規定した上で、乱数系列を指定するデータ (乱数初期値) を設定

・送信しても構わない。

図7は図1のスクランブラ100の変形例である。スクランブラ700ではスクランブラ100のスクランブル処理を3回直列に施しており、それぞれのスクランブル部701, 702, 703において必ず異なる位置のデータを換字処理する。異なる位置を指定する場合には、例えば、直近のスタートコード位置から換字位置までのバイト数を4で割った時、スクランブル部701では余りが0に、702では余りは1に、703では余りは2になるように換字位置を指定するよことにより実現できる。このようにして生成したスクランブルストリーム710は、正しく再生するためには、鍵715, 725, 735にそれぞれ対応する3つの鍵が必要となる。しかし、取得した鍵の個数が0個、1個、2個の場合にも部分視聴が可能で、しかも取得した鍵の数が多いほど劣化の少ない画像を視聴することができる。

#### 【0024】

また、鍵毎にスクランブルの強度を変えておくと、例えば3個の鍵の有無にて、正常な視聴も含め8通りのスクランブルを実現できる。複数の鍵は、例えばあるグループには第1の鍵を、別のグループには、スクランブル強度の異なる第2の鍵を渡しておけば、グループ毎に異なるスクランブル強度を提供することができる。

上記の説明ではいずれも、ヘッダ部分としては、映像ストリームすなわちエレメンタリストリームのヘッダ部分を前提にしていたが、映像ストリーム以外のデータを多重したストリームにおいて、以下の変形例も本願に含まれることは明白である。

映像ストリームと音声ストリームをシステムレイヤを用いて多重化したストリームの場合、映像ストリームのみを抽出し、スクランブルを適用し、スクランブル後のストリームを元の多重化データに書き戻す方法である。このとき、ストリームの総データ数は変わらないため、書き戻し処理は単純にもとのデータを上書きするだけでよい。すなわち、元の多重化されたストリームの置換位置のデータを変更すればよい。もし、システムレイヤにおいて、データ誤り防止のためストリームのパリティ・誤り訂正符号等を併記している場合は、パリティ・誤り訂正符

号等を再計算修正して書き換えれば、データとしての整合性を保つことができる。なお、送信、受信双方において事前に取り決めることにより、上記パリティ・誤り訂正符号等を修正しない、すなわち、受信側にてパリティ・誤り訂正符号等を参照しないことも可能である。

## 【 0 0 2 5 】

映像ストリームと音声ストリームをシステムレイヤを用いて多重化したストリームの場合、保護する（上記の説明において「ヘッダ」に該当する）部分を、システムレイヤデータと映像ストリームのヘッダと音声ストリームとして扱うことにより、映像ストリームに対する処理を多重化されたシステムストリームに直接適用することが可能である。この場合、データ解析部 2 0 2 においては、システムレイヤのシンタックスを解析し、処理しているデータがシステムレイヤ、映像ストリーム、音声ストリームのいずれに属するかを判定する。処理しているデータがシステムレイヤあるいは音声ストリームの場合は置換処理を禁止（データを保護）し、映像ストリームの場合は映像ストリームのヘッダ部を識別し、先に説明した方法により保護／置換を判定する。

## 【 0 0 2 6 】

このような多重されたデータの場合は、本発明のスクランブラを複数使用することができる。すなわち、多重されているエレメンタリストリーム（映像あるいは音声・オーディオがそれぞれ 0 以上、合計 2 ストリーム以上が多重）のうち、2 つ以上に独立した置換処理を適用する。具体的には、本発明を適用する処理しているデータの種類により独立したスクランブルパラメータ A、B、C を切り替える方法である。この場合、同一のパラメータを用いて独立の処理を行うことも可能であり、スクランブルパラメータを送付するデータ量を削減することができる。

## 【 0 0 2 7 】

なお、音声あるいはオーディオに対するスクランブルは、本発明と同様な置換処理にて実施することが可能である。この場合、ヘッダを保護する必要はない。

図 8 は図 1 のスクランブラ 1 0 0 を用いた映像配信システムの応用例である。こ



ここで映像ストリームは同報配信を想定している。すなわち、同一のストリームを希望する受信機全員に配信し、受信者のうち、鍵を入手した端末のみが正しく映像を視聴することができる。また、スクランブルパラメータ 1 2 3 は定期的に出され、映像ストリーム 1 1 3 に多重して伝送される。ここで、スクランブルパラメータ 1 2 3 が多重された直後の映像ストリーム 1 1 3 はランダムアクセスポイント（ストリームの途中から視聴を開始できるポイント）である。

## 【 0 0 2 8 】

図 8 にて、端末 8 1 1 のユーザは送受信機 8 1 0 経由で WEB サーバ 8 3 0 にアクセスし、視聴可能な映像の情報を得る。この時の情報としては、映像のスナップショット、テキストによる説明、視聴方法、視聴料金等が含まれる。ユーザが映像ストリーム 1 1 1 の視聴希望した場合は、同報送信中の映像ストリーム 1 1 3 の視聴を開始し、これと並行し WEB サーバ 8 3 0 経由で、鍵取得希望を送出する。この時、料金を支払うための ID 番号、パスワードや、クレジットカード番号等を送出してもかまわない。WEB サーバ 8 3 0 はユーザの鍵取得要求の妥当性を確認するために、認証サーバ 8 4 0 へ問い合わせる。この問い合わせの内容は、例えばユーザ ID とパスワードの妥当性であったり、クレジットカードの有効性の確認であったりする。記憶手段に予め記憶されるユーザ情報を用いて判定を行い、該ユーザの妥当性が確認できると、WEB サーバは鍵管理サーバ 8 2 0 に対し、映像ストリーム 1 1 1 をスクランブルする時に用いた鍵 1 3 1 に対応する解読鍵取得を要求する。この時に、認証サーバ 8 4 0 が発行するデジタル証明書等を添付しても構わない。鍵管理サーバ 8 2 0 より解読鍵を得た WEB サーバは鍵情報を端末 8 1 1 に送信する。端末 8 1 1 では、解読鍵を用いてスクランブルストリーム 1 1 3 を解読し、正しい映像を視聴することができる。

## 【 0 0 2 9 】

図 8 の変形例としては、ユーザの妥当性を確認するために、ユーザが店舗等で購入した証明（例えば、レシート等に記載された ID コード等）を用いても構わない。この場合、図 8 の認証サーバ 8 4 0 は、店舗の P O S システム等と接続し、ユーザの購入データ、購入額等を確認した上で、認証を行う。

## 【 0 0 3 0 】

図 8 の別の変形例としては、コンテンツ毎に異なるスクランブルパラメータを与える例がある。すなわち、スクランブル装置に、入力するコンテンツと、入力するコンテンツに対応したスクランブル指示情報を入力し、スクランブル指示情報から所定の手段によりスクランブルパラメータを決定し、このスクランブルパラメータを用いてコンテンツ毎に異なるスクランブルをかける方法である。

具体的には、スクランブル指示情報として、スクランブルレベル 0 ～ 4 の整数値を用意し、スクランブルレベル 0 が指定された時は、スクランブルなし、1 ～ 3 の時は部分視聴の度合いの異なるスクランブル（1 がより、3 がより画質劣化が大きい）、そして 4 が完全スクランブル（部分視聴なし）とする。ここで、完全スクランブルの時は、一般の暗号を用いて、コンテンツの保護の強度を上げても構わないし、本発明手法のパラメータ A、B を極端に小さくして、部分視聴できない程度に画質を劣化させてもかまわない。

スクランブル指示情報として 1 ～ 3 が指示されたときには、スクランブル装置は予め用意されていたスクランブルパラメータ（主に A、B の値）を選択する。なお、このとき、先に示した入力ストリームの検査を実施し、その検査結果によりスクランブルパラメータを修正すればより適切な部分視聴映像が期待できる。本構成によれば、例えば店舗の販売等の景品として、映像視聴の鍵を与えることにより、コンテンツの視聴が可能となり、店舗の販売の促進効果が期待できる。また、鍵を持っていない顧客でも映像を部分視聴できるため、顧客が映像を正しく見たいために、店舗において物品を購入することを促す効果が期待できる。

#### 【 0 0 3 1 】

##### 【発明の効果】

本発明のコンテンツをスクランブルする機能によれば、暗号鍵を有する端末には正しい映像再生を行い、暗号鍵を持たない端末においては、映像コンテンツの一部あるいは画質の劣化したコンテンツが視聴（部分視聴）される。この時、スクランブルをかけるのは映像符号化の後に実施することができ、エンコードする者とスクランブルする者が別の者であることも可能となる。スクランブルのパラメータを選択してスクランブルの強度を選択することができる。

さらに、多段でのスクランブルを行う構成によれば、複数の鍵を用いるため、受

信者が取得する鍵の個数・組み合わせにより、部分視聴できる映像の画質を変えることができる。

【図面の簡単な説明】

【図 1】

本発明による第 1 の実施例を説明する図である。

【図 2】

スクランブル部の詳細説明図である。

【図 3】

スクランブル可否を決定するための状態遷移図を説明する図である。

【図 4】

ソフトウェアにて実装した場合のフローチャートである

【図 5】

換字表の例である。

【図 6】

換字表生成アルゴリズムの例である。

【図 7】

図 1 のスクランブラの変形例である。

【図 8】

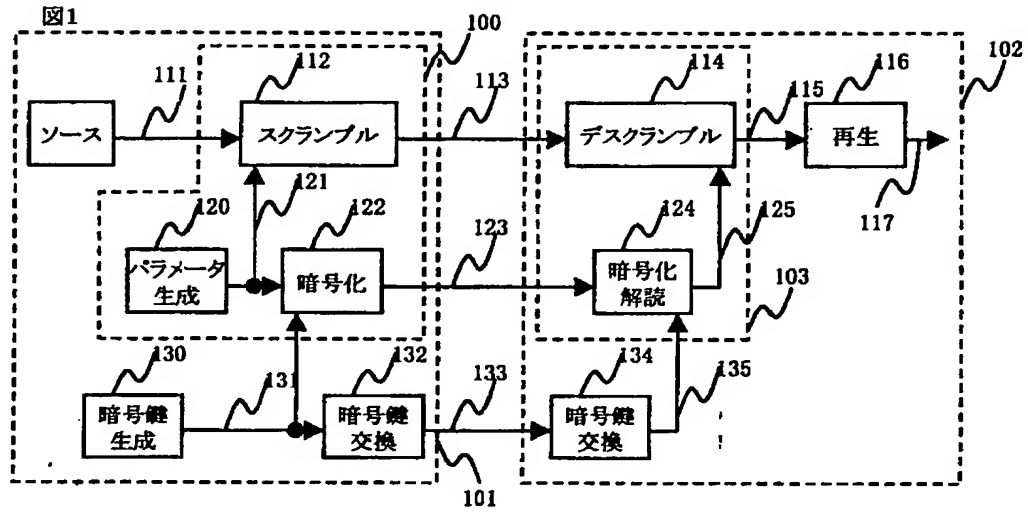
図 1 のスクランブラ 1 0 0 を用いた映像配信システムの応用例である。

【符号の説明】

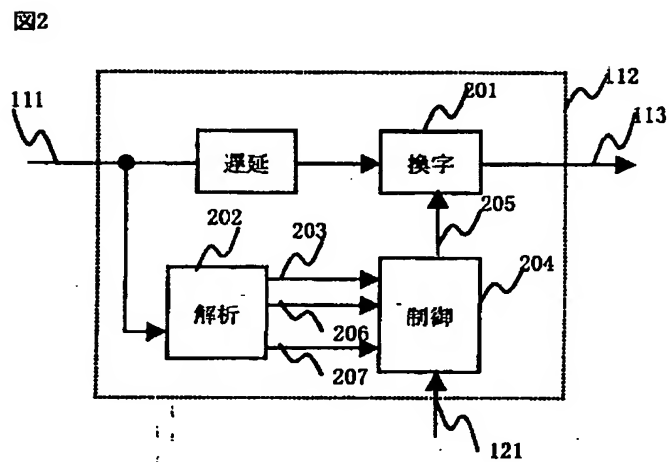
- 1 0 0、スクランブラ
- 1 0 3、デスクランブラ
- 1 1 2、スクランブル部
- 1 1 3、スクランブルストリーム
- 1 1 4、デスクランブル部
- 1 3 1、暗号鍵
- 1 2 3、秘置スクランブルデータ
- 2 0 1、換字処理。

【書類名】 図面

【図 1】

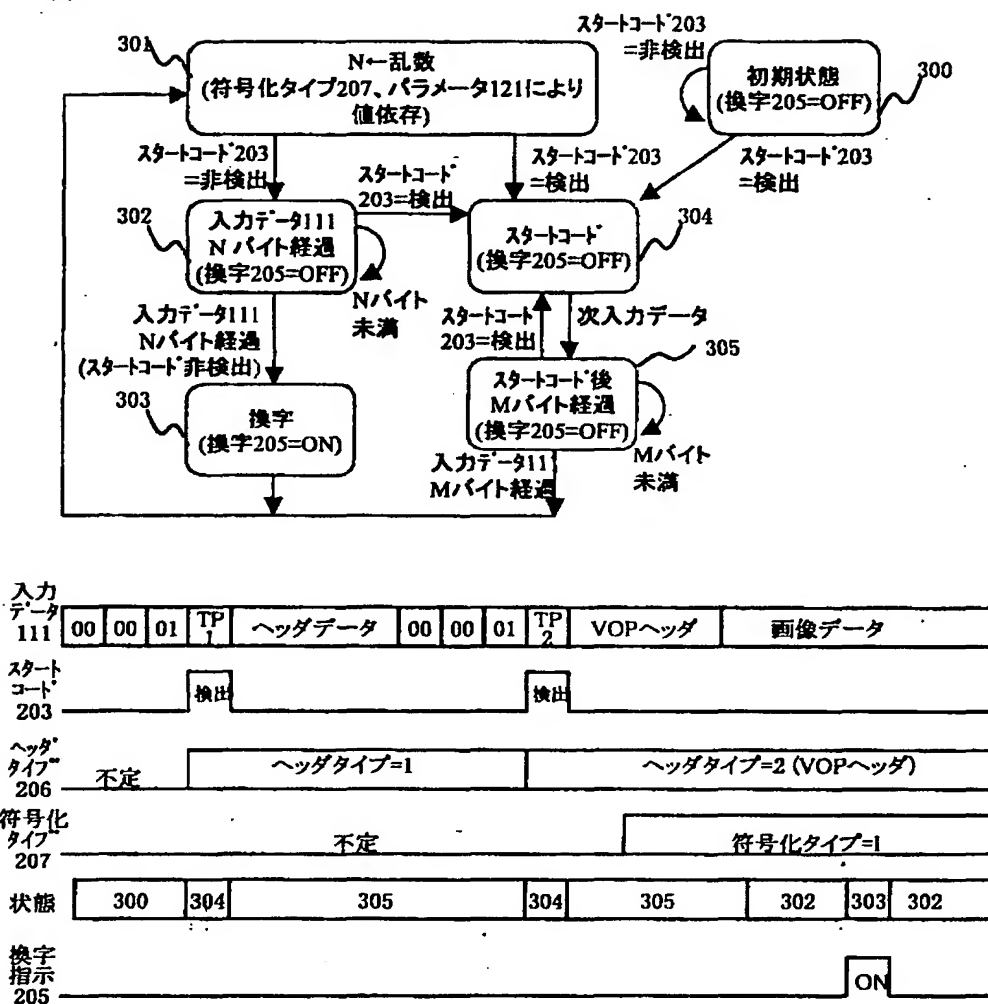


【図 2】



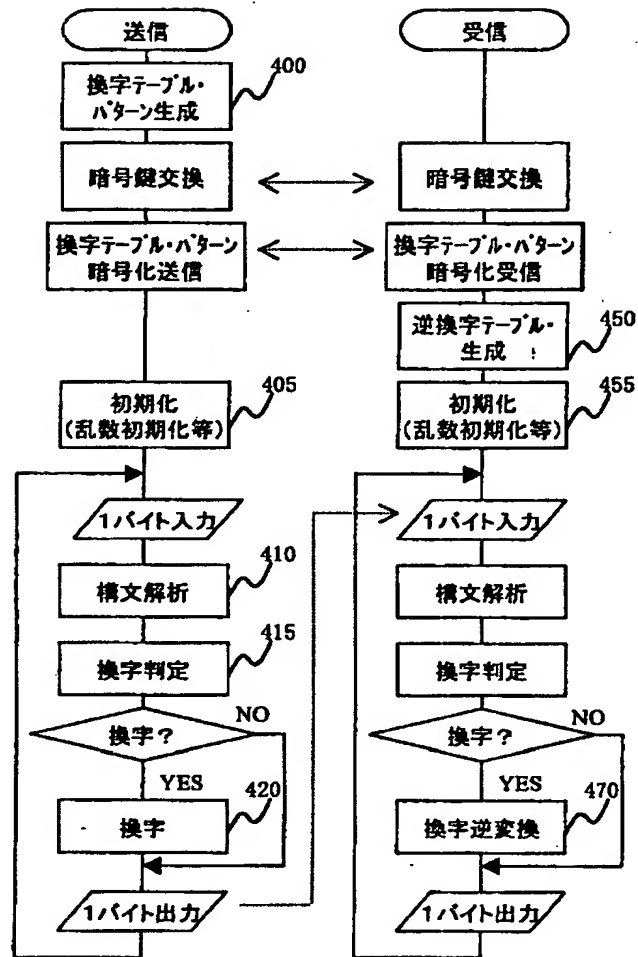
【图 3】

图3



【図 4】

図4

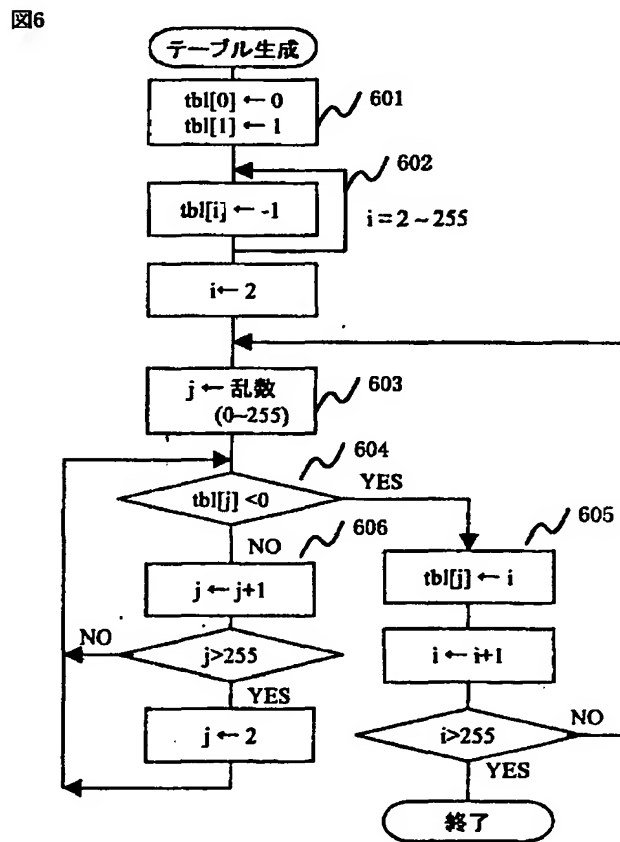


【図 5】

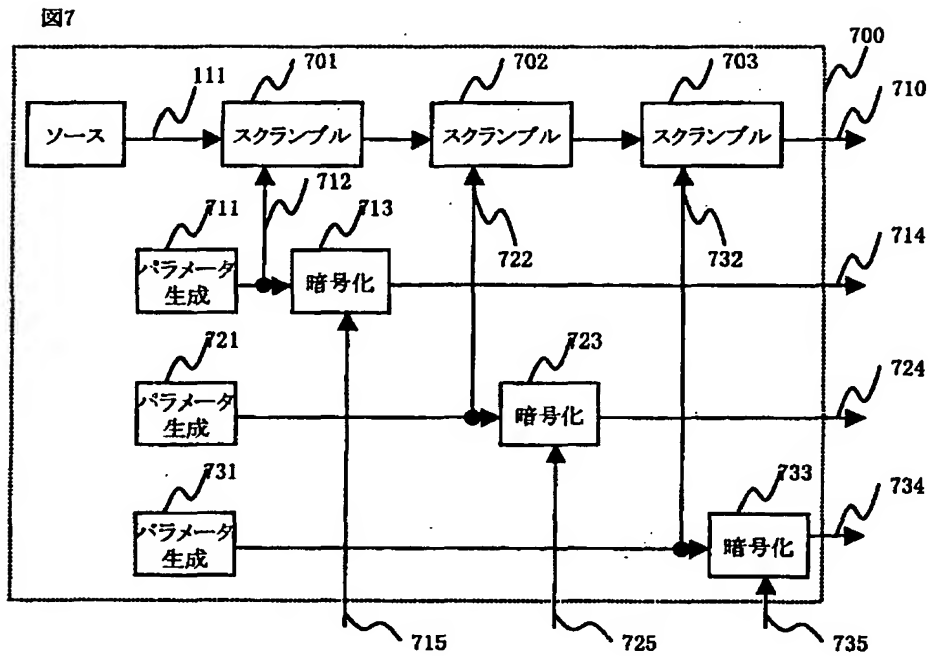
図5

番号	入力	出力
0	0000 0000	0000 0000
1	0000 0001	0000 0001
2	0000 0010	1011 0100
3	0000 0011	0010 1010
4	0000 0100	0011 0010
5	0000 0101	1110 0011
254	1111 1110	0110 0001
255	1111 1111	1001 0111

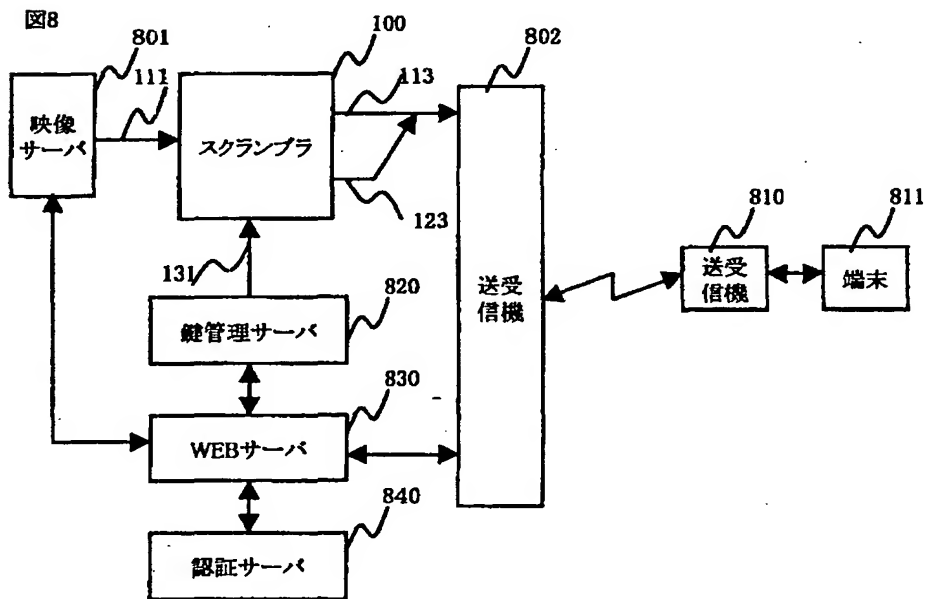
【図 6】



【図7】



【図8】





【書類名】 要約書

【要約】

【課題】従来は、映像コンテンツに対し、部分的な視聴を可能とするスクランブルをかける時、配信中継者がスクランブルをかけたり、符号化時と異なる強度のスクランブルをかけることができなかった。

【解決手段】上記目的を達成するために、符号化された映像コンテンツの画像データ部分の一部を暗号化することにより実現する。

【効果】上記手段により、コンテンツをスクランブルする機能が提供され、暗号鍵を有する端末には正しい映像再生を行い、暗号鍵を持たない端末においては、映像コンテンツの一部あるいは画質の劣化したコンテンツが視聴（部分視聴）される。この時、スクランブルをかけるのは映像符号化の後に実施することができ、エンコードする者とスクランブルする者が別の者であることも可能となる。スクランブルのパラメータを選択してスクランブルの強度を選択することができる。

【選択図】 図 1

認定・付加情報

特許出願の番号	特願 2 0 0 2 - 3 0 5 2 8 8
受付番号	5 0 2 0 1 5 7 6 5 7 0
書類名	特許願
担当官	第八担当上席 0 0 9 7
作成日	平成 1 4 年 1 0 月 2 2 日

<認定情報・付加情報>

【提出日】	平成14年10月21日
-------	-------------

出 願 人 履 歴 情 報

識別番号 [000005108]

1. 変更年月日	1990年 8月31日
[変更理由]	新規登録
住 所	東京都千代田区神田駿河台4丁目6番地
氏 名	株式会社日立製作所

INFORMATION UNDER 37 CFR 1.56(a)

(For Initial Filing)

The following references are submitted as information  
to comply with the duty of disclosure under 37 CFR 1.56(a):

References	Disclosed in the specification?		Copy			Translation	
	Yes	No	Enc.	Follow	Please obtain	Enc.	Not avail-able
1. JP-A-10-145772	<input type="radio"/>		<input type="radio"/>			<input type="radio"/> (only abstract)	
2.							
3.							
4.							
5.							
6.							
7.							

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-145772

(43)Date of publication of application : 29.05.1998

(51)Int.Cl. H04N 7/167  
H04K 1/04

(21)Application number : 08-295162 (71)Applicant : NEC CORP

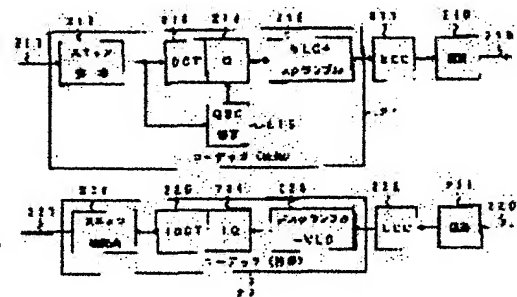
(22)Date of filing : 07.11.1996 (72)Inventor : ITOI TETSUSHI

## (54) METHOD FOR TRANSMITTING VIDEO, METHOD FOR RECEIVING VIDEO, VIDEO TRANSMITTER AND VIDEO RECEIVER

## (57)Abstract:

PROBLEM TO BE SOLVED: To induce a person without a contract to desire to look and listen a perfect video and sound by having a contract.

SOLUTION: On a transmitting side, when scanning transformation 212, DCT (discrete cosine transformation) transformation 213, quantization 214 and coded amount control 215 are performed and then variable coding 216 is performed on an original picture 211, it is variable-length-transformed and encoded as it is without scrambling in its low frequency component, and using another variable length table having the same number of bits in its high frequency component. Then, an error correcting code(ECC) 217 is added thereto and they are modulated 218 and obtaining a transmitting signal 219. On a receiving side, a contractor who has a scramble decoder performs variable length decoding 233 with a right table, so that a perfect reproducing picture 227 is restored. But an uncontractor who has no scramble decoder performs variable length decoding using a table having an erroneous high frequency component, so that a defective reproducing picture 227 is restored.



## LEGAL STATUS

[Date of request for examination] 07.11.1996

[Date of sending the examiner's decision of rejection] 23.02.2000

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]	3283771
[Date of registration]	01.03.2002
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

Copyright (C); 1998,2000 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-145772

(43) 公開日 平成10年(1998) 5月29日

(51) IntCl.<sup>6</sup>

識別記号

F I

H 0 4 N 7/167

H 0 4 N 7/167

Z

H 0 4 K 1/04

H 0 4 K 1/04

審査請求 有 請求項の数34 O L (全 16 頁)

(21) 出願番号 特願平8-295162

(22) 出願日 平成8年(1996)11月7日

(71) 出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(72) 発明者 糸井 哲史

東京都港区芝五丁目7番1号 日本電気株式会社内

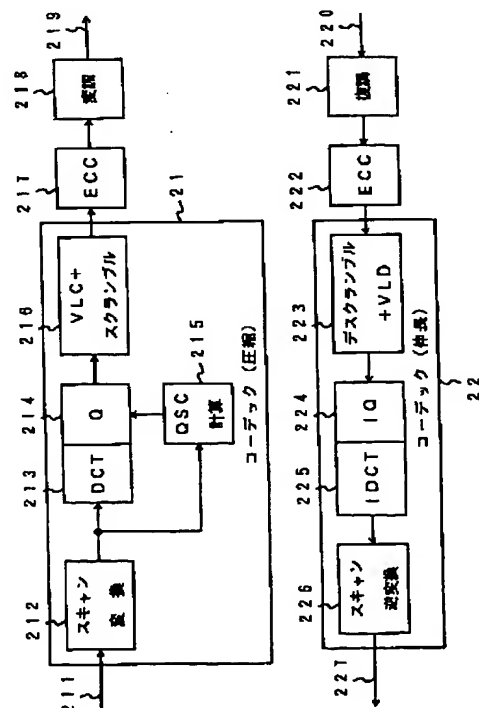
(74) 代理人 弁理士 後藤 洋介 (外2名)

(54) 【発明の名称】 映像送信方法および映像受信方法、映像送信装置および映像受信装置

(57) 【要約】

【課題】 未契約者にとって契約して完全な映像／音声を視聴したくなるようにすること。

【解決手段】 送信側で、原画像211に対し、スキャン変換212、DCT変換213、量子化214、符号量制御215した後、可変長符号化216する際、低周波成分にはスクランブルを掛けずにそのまま、高周波成分には同じビット数をもつ他の可変長テーブルを使用して可変長変換することにより符号化し、ECC217を付加し、変調218して送信信号219を得る。受信側では、スクランブルデコーダを持つ契約者は正しいテーブルで可変長復号化233することにより、完全な再生画像227を復元できる。スクランブルデコーダを持たない未契約者は233で低周波成分を正しいテーブルで、高周波成分を誤ったテーブルで可変長復号化することにより、不完全な再生画像227が復元される。



**【特許請求の範囲】**

【請求項 1】 原映像信号を圧縮して、圧縮映像信号を送信する映像送信方法において、前記圧縮映像信号に対して軟らかいスクランブルを掛けて得られる信号を送信信号として送信すること、を特徴とする映像送信方法。

【請求項 2】 前記軟らかいスクランブルは、受信側でデスクランブルしない場合に多少の絵柄が判別できる程度に前記原映像信号を再生できるようにスクランブルすること、である請求項 1 に記載の映像送信方法。

【請求項 3】 請求項 1 又は 2 に記載の映像送信方法で得られる送信信号を受信信号として受信する映像受信方法であって、

前記受信信号に対して前記軟らかいスクランブルの逆変換である軟らかいデスクランブルを掛けることにより、前記圧縮映像信号を復元し、この復元した圧縮映像信号を伸長して前記原映像信号を再生することを特徴とする映像受信方法。

【請求項 4】 前記圧縮映像信号は、前記原映像信号を直交変換した後、量子化、可変長符号化することにより得られる映像信号である、請求項 1 に記載の映像送信方法。

【請求項 5】 請求項 4 に記載の映像送信方法で得られる送信信号を受信信号として受信する映像受信方法であって、

前記受信信号に対して前記軟らかいスクランブルの逆変換である軟らかいデスクランブルを掛けることにより、前記圧縮映像信号を復元し、

この復元した圧縮映像信号を伸長して前記原映像信号を再生し、

前記伸長が、前記復元した圧縮映像信号を可変長復号化し、逆量子化し、および逆直交変換することである映像受信方法。

【請求項 6】 前記軟らかいスクランブルは、各直交変換ブロックにおいて低周波成分にはスクランブルを掛けず、高周波成分にはスクランブルを掛けること、である請求項 4 に記載の映像送信方法。

【請求項 7】 前記軟らかいスクランブルは、全成分を高周波成分とみなしてスクランブルを掛けること、である請求項 6 に記載の映像送信方法。

【請求項 8】 スクランブルを掛けない低周波成分を、直流成分のみとすること、を特徴とする請求項 6 に記載の映像送信方法。

【請求項 9】 スクランブルを掛けない低周波成分を、直流成分と低周波側から規定された個数のラン／レベルの組み合わせとすること、を特徴とする請求項 6 に記載の映像送信方法。

【請求項 10】 スクランブルを掛ける高周波成分を、エンドオブブロック側の低周波側から低周波側に向かって規定された個数のラン／レベルの組み合わせとすること、を特徴とする請求項 6 に記載の映像送信方法。

【請求項 11】 可変長テーブルにおいて、変換した後同じビット数をもつ他のテーブルを使用した可変長変換することによりスクランブルを掛けること、を特徴とする請求項 6 に記載の映像送信方法。

【請求項 12】 本来のテーブルと、同じビット数をもつ別のテーブルとのテーブル上での距離をスクランブルデータから求めること、を特徴とする請求項 11 に記載の映像送信方法。

【請求項 13】 原映像信号を圧縮して、圧縮映像信号を送信する映像送信方法において、前記原映像信号を圧縮する前に、前記原映像信号に対して軟らかいスクランブルを掛けること、を特徴とする映像送信方法。

【請求項 14】 前記軟らかいスクランブルは、受信側でデスクランブルしない場合に多少の絵柄が判別できる程度に前記原映像信号を再生できるようにスクランブルすること、である請求項 13 に記載の映像送信方法。

【請求項 15】 前記軟らかいスクランブルは、前記原映像信号に対して、所定の塊内で所定のブロック単位を特定の順序で並べ変えること、である請求項 13 に記載の映像送信方法。

【請求項 16】 前記軟らかいスクランブルは、グループオブピクチャー内でピクチャーデータを特定の順序で並べ変えること、である請求項 13 に記載の映像送信方法。

【請求項 17】 前記軟らかいスクランブルは、ピクチャー内でスライスデータを特定の順序で並べ変えること、である請求項 13 に記載の映像送信方法。

【請求項 18】 前記軟らかいスクランブルは、スライス内でマイクロブロックデータを特定の順序で並べ変えること、である請求項 13 に記載の映像送信方法。

【請求項 19】 前記軟らかいスクランブルは、グループオブピクチャー内でピクチャーデータを特定の順序で並べ変えること、ピクチャー内でスライスデータを特定の順序で並べ変えること、およびスライス内でマイクロブロックデータを特定の順序で並べ変えること、のうち少なくとも 2 つを組み合わせること、である請求項 13 に記載の映像送信方法。

【請求項 20】 請求項 13 に記載の映像送信方法で得られる送信信号を受信信号として受信する映像受信方法であって、

前記受信信号を伸長して前記軟らかいスクランブルを掛けて得られるスクランブル済信号を復元し、

前記スクランブル済信号に対して前記軟らかいスクランブルの逆変換である軟らかいデスクランブルを掛けることにより、前記原映像信号を再生することを特徴とする映像受信方法。

【請求項 21】 原映像信号を圧縮して、圧縮映像信号を送信する映像送信方法において、前記原映像信号を圧縮する前に、前記原映像信号に対して軟らかい主スクランブルを掛け、前記圧縮映像信号に対して軟らかい副ス



スクランブルを掛けて得られる信号を送信信号として送信すること、を特徴とする映像送信方法。

【請求項 22】 前記圧縮映像信号は、前記原映像信号を直交変換した後、量子化、可変長符号化することにより得られる映像信号であり、

前記軟らかい主スクランブルは、前記原映像信号に対して、所定の塊内で所定のブロック単位を特定の順序で並べ変えることであり、

前記軟らかい副スクランブルは、各直交変換ブロックにおいて低周波成分にはスクランブルを掛けず、高周波成分にはスクランブルを掛けること、である請求項 21 に記載の映像送信方法。

【請求項 23】 前記軟らかい主スクランブルは、グループオブピクチャー内でピクチャーデータを特定の順序で並べ変えること、ピクチャー内でスライスデータを特定の順序で並べ変えること、およびスライス内でマイクロブロックデータを特定の順序で並べ変えること、のうちから選択された少なくとも 1 つである請求項 21 に記載の映像送信方法。

【請求項 24】 請求項 21 に記載の映像送信方法で得られる送信信号を受信信号として受信する映像受信方法であって、

前記受信信号に対して前記軟らかい副スクランブルの逆変換である軟らかい副デスクランブルを掛けることにより、前記圧縮映像信号を復元し、

この復元した圧縮映像信号を伸長して前記軟らかい主スクランブルを掛けて得られる主スクランブル済信号を復元し、

前記主スクランブル済信号に対して前記軟らかい主スクランブルの逆変換である軟らかい主デスクランブルを掛けることにより、前記原映像信号を再生することを特徴とする映像受信方法。

【請求項 25】 原映像信号を圧縮して圧縮映像信号を得る圧縮手段と、

前記圧縮映像信号に対して軟らかいスクランブルを掛けて得られる信号を送信信号として送信するスクランブル手段とを有することを特徴とする映像送信装置。

【請求項 26】 前記圧縮手段は、前記原映像信号を直交変換して直交変換した信号を出力する直交変換手段と、該直交変換した信号を量子化して量子化した信号を出力する量子化手段と、該量子化した信号を可変長符号化することにより前記圧縮映像信号を得る可変長符号化手段とを有し、

前記スクランブル手段は、各直交変換ブロックにおいて低周波成分にはスクランブルを掛けず、高周波成分にはスクランブルを掛けることにより前記軟らかいスクランブルを実行する請求項 25 に記載の映像送信装置。

【請求項 27】 請求項 25 に記載の映像送信装置で得られた送信信号を受信信号として受信する映像受信装置であって、

前記受信信号に対して前記軟らかいスクランブルの逆変換である軟らかいデスクランブルを掛けることにより、前記圧縮映像信号を復元するデスクランブル手段と、この復元した圧縮映像信号を伸長して前記原映像信号を再生する伸長手段とを有することを特徴とする映像受信装置。

【請求項 28】 原映像信号に対して軟らかいスクランブルを掛けてスクランブル済信号を得るスクランブル手段と、

該スクランブル済信号を圧縮して圧縮映像信号を得る圧縮手段とを有し、

前記圧縮映像信号を送信信号として送信することを特徴とする映像送信装置。

【請求項 29】 前記スクランブル手段は、前記原映像信号に対して、所定の塊内で所定のブロック単位を特定の順序で並べ変えることにより前記軟らかいスクランブルを実行し、

前記圧縮手段は、前記スクランブル済信号を直交変換して直交変換した信号を出力する直交変換手段と、該直交変換した信号を量子化して量子化した信号を出力する量子化手段と、該量子化した信号を可変長符号化することにより前記圧縮映像信号を得る可変長符号化手段とを有すること、を特徴とする請求項 28 に記載の映像送信装置。

【請求項 30】 請求項 28 に記載の映像送信装置で得られた送信信号を受信信号として受信する映像受信装置であって、

前記受信信号を伸長して前記軟らかいスクランブルを掛けて得られるスクランブル済信号を復元する伸長手段と、

その復元されたスクランブル済信号に対して前記軟らかいスクランブルの逆変換である軟らかいデスクランブルを掛けることにより、前記原映像信号を再生するデスクランブル手段とを有することを特徴とする映像受信装置。

【請求項 31】 原映像信号に対して軟らかいスクランブルを掛けて主スクランブル済信号を得る主スクランブル手段と、

該主スクランブル済信号を圧縮して圧縮映像信号を得る圧縮手段と、

前記圧縮映像信号に対して軟らかい副スクランブルを掛けて副スクランブル済信号を得る副スクランブル手段とを有し、前記副スクランブル済信号を送信信号として送信することを特徴とする映像送信装置。

【請求項 32】 前記主スクランブル手段は、前記原映像信号に対して、所定の塊内で所定のブロック単位を特定の順序で並べ変えることにより前記軟らかい主スクランブルを実行し、

前記圧縮手段は、前記主スクランブル済信号を直交変換して直交変換した信号を出力する直交変換手段と、該直

交変換した信号を量子化して量子化した信号を出力する量子化手段と、該量子化した信号を可変長符号化することにより前記圧縮映像信号を得る可変長符号化手段とを有し、

前記副スクランブル手段は、前記各直交変換ブロックにおいて低周波成分にはスクランブルを掛けず、高周波成分にはスクランブルを掛けることにより前記軟らかい副スクランブルを実行する請求項 31 に記載の映像送信装置。

【請求項 33】 前記主スクランブル手段は、グループオブピクチャー内でピクチャーデータを特定の順序で並べ変えること、ピクチャー内でスライスデータを特定の順序で並べ変えること、およびスライス内でマイクロブロックデータを特定の順序で並べ変えること、のうちから選択された少なくとも 1 つを実行する請求項 32 に記載の映像送信方法。

【請求項 34】 請求項 31 に記載の映像送信装置で得られる送信信号を受信信号として受信する映像受信装置であって、

前記受信信号に対して前記軟らかい副スクランブルの逆変換である軟らかい副デスクランブルを掛けることにより、前記圧縮映像信号を復元する副デスクランブル手段と、

この復元した圧縮映像信号を伸長して前記主スクランブル済信号を復元する伸長手段と、

この復元した主スクランブル済信号に対して前記軟らかい主スクランブルの逆変換である軟らかい主デスクランブルを掛けることにより、前記原映像信号を再生する主デスクランブル手段とを有することを特徴とする映像受信装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明はディジタルテレビジョン放送に好適なスクランブル方式および装置に関する。

【0002】

【従来の技術】図 17 に従来のディジタルテレビジョン放送における信号処理ブロック（映像送信装置と映像受信装置）を示す。映像送信装置はコーデック（圧縮）ブロック 11 と、スクランブル回路 117' と、ECC 付加回路 118 と、変調回路 119 とを有する。コーデック（圧縮）ブロック 11 は、スキャン変換回路 112 と、DCT 変換回路 113 と、量子化回路 114 と、符号量制御回路 115 と、可変長符号化（VLC）回路 116 とを有する。

【0003】映像送信装置では、原画像（原映像信号）111 に対し、コーデック（圧縮）ブロック 11 において、スキャン変換回路 112 でスキャン変換し、DCT 変換回路 113 で DCT 変換し、量子化回路 114 で量子化し、符号量制御回路 115 で符号量制御を行い、可

変長符号化回路 116 で可変長符号化することによって、圧縮映像信号を得ている。さらに、この圧縮映像信号に対してスクランブル回路 117' でスクランブルを掛け、ECC 付加回路 118 で ECC を付加し、変調回路 119 で変調して送信信号 120 を得る。

【0004】一方、映像受信装置は、復調回路 122 と、ECC 処理回路 123 と、デスクランブル回路 124' と、コーデック（伸長）回路 12 とを有する。コーデック（伸長）回路 12 は、可変長復号化（VLD）回路 125 と、逆量子化回路 126 と、逆 DCT 変換回路 127 と、スキャン逆変換回路 128 とを有する。

【0005】映像受信装置では、受信信号 121 を復調回路 122 で復調し、ECC 処理回路 123 で ECC 処理を行い、スクランブルデコーダを持つ契約者はデスクランブル回路 124' で正しいデスクランブルを行って、デスクランブルされた信号（圧縮映像信号）を得る。さらに、コーデック（伸長）回路 12 において、デスクランブルされた信号（圧縮映像信号）を可変長復号化回路 125 で可変長復号化し、逆量子化回路 126 で逆量子化し、逆 DCT 変換回路 127 で逆 DCT し、スキャン逆変換回路 128 でスキャン逆変換することにより、再生画像 129 を復元する。

【0006】尚、スクランブルブロックと ECC ブロック（スクランブル回路 117' と ECC 付加回路 118 およびデスクランブル回路 124' と ECC 処理回路 123）は入れ替えも可能である。

【0007】ここで、スクランブル回路 117' におけるスクランブルに関しては種々の方法が提案されているが、最も簡単なのは特定の生成多項式により発生したランダムデータを映像／音声などの伝送すべきデータに Mod 2 加算する方法である。例えば生成多項式を、下記の数式 1

【0008】

【数 1】

$$g(X) = X^{15} + X + 1$$

とし、プリセットデータを全ビット“1”としてランダムデータを発生する方法がある。

【0009】受信契約者には上記数式 1 で表される生成多項式によるデスクランブル（スクランブル解読）回路 124' を配布することにより、契約者は正常な映像／音声などの伝送すべきデータを得ることができる。しかし、受信契約をしていないと、上記数式 1 で表される生成多項式が分からず、スクランブルされた全く意味のないデータのみ得られ、正常な映像／音声などの伝送すべきデータは得られない。ここでは、全く意味のないデータにスクランブルすることを、「硬くスクランブルする」と呼ぶことにする。また、硬くスクランブルすることを、完全に又は強くスクランブルするとも呼ぶ。すなわち、従来のスクランブル回路 117' は、圧縮映像信号に対して硬い（完全なまたは強い）スクランブルを掛

けている。

【0010】本発明に関連する先行技術が種々知られている。例えば、特開平 7 - 1 1 1 6 4 7 号公報（以下、先行技術 1 と呼ぶ）は、映像データの再生に際して、その再生者を限定するためのスクランブル装置に関するもので、目的に応じて見え方を制御できるスクランブルおよびデスクランブル処理を行うようにした「信号処理装置」を開示している。先行技術 1 において、原信号は、MPEG 標準に準拠した映像信号であり、コード検出装置は、各符号を読み取り、“det type” 信号を検出し、検出信号を乱数発生装置へ送る。乱数発生装置は、スクランブル鍵に基づいて乱数生成し、排他的論理和回路を介して、乱数発生装置からの信号を原信号に排他的論理和演算してスクランブル信号を得る。再生側は、同じ構成で逆変換処理する。このような構成により、スクランブル効果制御以外にも、単に特殊効果としても利用可能となる。

【0011】また、特開平 7 - 6 7 0 9 6 号公報（以下、先行技術 2 と呼ぶ）は、映像データの再生に際して、その再生者を限定するためのスクランブル装置に関するもので、スクランブルデータが予約語と一致することによる再生器の誤動作を防止するようにした「スクランブル装置」を開示している。先行技術 2 において、符号検出装置では、入力される MPEG に準拠した画像データについて入力されてくる信号を読み取り、スクランブルした場合に予約語と一致することがない部分をスクランブルの対象として検出し、スクランブル命令を乱数発生器に伝送する。乱数発生器は、符号検出回路からのスクランブル命令があるときのみ乱数を発生し、データに排他的論理和演算を行う。再生側は、その逆変換を行う。

【0012】さらに、特開昭 4 - 8 0 2 9 号公報（以下、先行技術 3 と呼ぶ）は、符号化方式における初期値のみを暗号鍵により暗号化し伝送することにより、秘密性が高く、暗号化部を低速処理し、ハードウェアを小型化し、コストの低廉化を実現するようにした「暗号化符号化装置」を開示している。先行技術 3 において、データ圧縮手段は 8 ビットのデジタル信号を 4 ビットの符号に圧縮する圧縮器で構成され、信号変換手段で変換された信号を符号化方式により圧縮して伝送する。暗号化手段は初期値のみに予め送受信者間で秘密に決めておいた 6 4 ビットの鍵により暗号化する。この初期値はテレビジョンの場合、1 走査線毎、あるいは数分の一走査線毎の初期値を与える為、この符号化データの初期値のみを暗号鍵により暗号化することで秘密性が保たれる。

【0013】特開昭 5 - 1 4 5 9 2 3 号公報（以下、先行技術 4 と呼ぶ）は、置換可能な機密保護モジュールを提案している。先行技術 4 において、プログラム信号はキーによりスクランブルされる。該キーは 2 度暗号化され、スクランブルされたプログラム信号と多重化され

る。復号器はその中に記憶された第 2 機密一連信号を用いて第 1 キー解読を実施し、次いで、置換可能機密保護モジュールの中に記憶された第 1 機密一連番号を用いて置換可能機密保護モジュールにより解読される。次いで、復号器は 2 回解読済みキーを用いてプログラムをデスクランブルする。

【0014】

【発明が解決しようとする課題】前述したように、従来のスクランブル方法では受信契約をしていない人たちにとっては硬く（完全に又は強く）スクランブルされた全く意味のないデータのみ得られる。

【0015】しかしながら、全く意味のないランダムデータよりもある程度概要が分かるくらいの映像が得られた方が、見ている人にとって契約して完全な映像／音声などを見たくなり、受信契約が増加すると言われている。

【0016】例えば、すでにアナログ放送においては WOW 放送で、ある程度概要が分かるくらいの映像を放送しており、それによる受信契約の増加という面でその効果が認められている。

【0017】また先行技術 1 および 2 は、乱数発生装置を用いてスクランブルを行うので、従来のスクランブル方法と同様に、スクランブルして得られたデータは全く意味のないデータである。先行技術 3 は符号化データの初期値のみを暗号鍵により暗号化し伝送する技術思想であって、スクランブルする技術思想とは異なる。さらに、先行技術 4 はプログラム信号をキーによりスクランブルする技術思想であって、本発明とはスクランブルしようとするデータが全く異なる。

【0018】したがって、本発明の目的は、未契約者にとって契約して完全な映像／音声を視聴したくなるようにすることにある。

【0019】

【課題を解決するための手段】本発明は上述した課題を解決したものであり、原映像信号を圧縮して、圧縮映像信号を送信する映像送信方法において、圧縮した後および／または前に圧縮映像信号および／または原映像信号に対して軟らかいスクランブルを掛けること、を特徴とする映像送信方法である。

【0020】ここで、「軟らかいスクランブル」とは、受信側でデスクランブルをしない場合に多少の絵柄が判別できる程度の原映像信号を再生できるようにスクランブルすることを言う。また、軟らかいスクランブルは、不完全なスクランブル又は弱いスクランブルとも呼ばれる。

【0021】その具体例としては、圧縮映像信号が原映像信号を直交変換した後、量子化、可変長符号化することにより得られた信号である場合、軟らかいスクランブルは、各直交変換ブロックにおいて低周波成分はスクランブルを掛けずに送信し、高周波成分はスクランブルを

掛けて送信することである。また、他の具体例としては、軟らかいスクランブルは、原映像信号に対して、所定の塊内で所定のブロック単位を特定の順序で並べ変える（シャフルする）ことである。なお、圧縮映像信号には、必要に応じて誤り訂正符号が付加されても良い。

#### 【0022】

【作用】受信側では、受信契約者がスクランブルデコーダによりデコードすれば全域データ、即ち完全な映像／音声などのデータが再生でき、受信契約をしていない人たちがスクランブルデコーダなしでデコードすれば多少の絵柄が判別できる程度の映像が再生できる。このことにより、受信契約者をしていない人たちの完全な映像／音声などを見たいという欲求を高め、受信契約を増加させることができる。

#### 【0023】

【発明の実施の形態】以下、本発明の実施の形態について図面を参照して詳細に説明する。

【0024】図1に本発明の一実施の形態（第1の実施例）による映像送信装置および映像受信装置とを示す。

【0025】映像送信装置は、コーデック（圧縮）ブロック21とECC付加回路217と変調回路218とを有する。コーデック（圧縮）ブロック21は、スキャン変換回路212とDCT変換回路213と量子化回路214と符号量制御回路215と可変長符号化（VLC）＋スクランブル回路216とを有する。

【0026】映像送信装置では、原画像（原映像信号）211に対し、コーデック（圧縮）ブロック21において直交変換＋量子化（Q）＋可変長符号化（VLC）による映像データ圧縮処理が行われる。直交変換の代表例として（動き補償）DCTがあり、圧縮フォーマットの代表例としてMPEG2方式がある。図1では、原画像（原映像信号）211をスキャン変換回路212でスキャン変換し、DCT変換回路213でDCT変換し、量子化回路214で量子化し、符号量制御回路215で符号量制御することを示している。その後、可変長符号化（VLC）＋スクランブル回路216によりVLCテーブル（図示せず）選択時にスクランブルが掛けられる。コーデック（圧縮）ブロック21の出力は、ECC付加回路217より誤り訂正符号が付加され、変調回路218によりデジタル放送特有の、例えばOFDM変調処理が施された後、送信映像データ219が得られる。

【0027】映像受信装置は、復調回路221とECC処理回路222とコーデック（伸長）ブロック22とを有する。コーデック（伸長）ブロック22は、デスクランブル＋可変長復号化（VLD）回路223と逆量子化回路224と逆DCT回路225とスキャン逆変換回路226とを有する。

【0028】映像受信装置では、受信信号220に対して復調回路221により例えばOFDM復調を施し、ECC処理回路222により符号誤り訂正処理が施された

後、コーデック（伸長）ブロック22で伸長処理が施される。ここで、スクランブルデコーダを持つ契約者はデスクランブル＋可変長復号化（VLD）回路223において正しいテーブルを使用して可変長復号化し、逆量子化回路224で逆量子化し、逆DCT回路225で逆DCT変換し、スキャン逆変換回路226でスキャン逆変換することにより完全な再生画像227が復元できる。これに対して、スクランブルデコーダを持たない未契約者はデスクランブル＋可変長復号化（VLD）回路223において低周波成分を正しいテーブルで、高周波成分を誤ったテーブルを使用して可変長復号化し、逆量子化回路224で逆量子化し、逆DCT回路225で逆DCT変換し、スキャン逆変換回路226でスキャン逆変換することにより不完全な再生画像227が復元される。

【0029】図2にVLC＋スクランブル回路216のブロック図を示す。VLC＋スクランブル回路216は、高域／低域成分分離回路32とタイミング調整用メモリ35とVLCシフト回路36とスクランブル回路37と統合回路38とを有する。

【0030】次に図2を参照して、VLC＋スクランブル回路216の動作について説明する。直交変換、量子化された映像データ31は高域／低域成分分離回路32により、低域成分33と高域成分34とに分離される。そして、高域成分34はVLCシフト回路36により、同じビット数を持つ他のテーブルデータが割り当てられる。どのテーブルデータが割り当てられるかは、スクランブル回路37の出力データにより決定される。低域成分33は、高域成分が上記処理を施されている間、タイミング調整用メモリ35により遅延される。タイミング調整用メモリ35により遅延された低域成分とVLCシフト回路36によりスクランブルされた高域成分は統合回路38で統合され、VLC＋スクランブル回路出力信号39としてECC回路217（図1）へ出力される。

【0031】図3にデスクランブル＋VLD回路223のブロック図を示す。デスクランブル＋VLD回路223は、高域／低域成分分離回路42と、タイミング調整用メモリ45とVLDシフト回路46とデスクランブル回路47と高域／低域成分統合回路48とを有する。

【0032】次に図3を参照して、デスクランブル＋VLD回路223の動作について説明する。ECC処理回路222（図1）から入力した映像データ41は、高域／低域成分分離回路42で低域成分43と高域成分44とに分離される。そして、高域成分44はVLDシフト回路46により同じビット数を持つスクランブルされる前のテーブルデータに変換され、可変長復号化される。スクランブルされる前のテーブルデータがどのテーブルデータかは、デスクランブル回路47の出力データにより決定される。低域成分43は、高域成分44が上記処理を施されている間、タイミング調整用メモリ45により遅延される。このタイミング調整用メモリ45で遅延

された低域成分とVLDシフト回路46によりデスクランブルされた高域成分とは高域/低域成分統合回路48で統合され、デスクランブル+VLD回路出力信号49として逆量子化回路224(図1)へ出力される。

### 【0033】

【実施例】次に、直交変換を4画素×4ラインを1ブロックとする2次元DCT変換とした場合について、送信側における具体的な例について説明する。

【0034】図4に、2次元DCT変換を行い、さらに量子化を行った後の行列データ31を示す。図4のデータをジグザグスキャンすると、順に、15, -2, 0, 0, 0, -1, 0, 0, -3, 0, 0, 2, 0, 1, 0, 0となる。これをハフマン符号により可変長符号化するため、ラン/レベルで示すと、DC=15, ラン=0/レベル=-2, ラン=3/レベル=-1, ラン=2/レベル=-3, ラン=2/レベル=2, ラン=1/レベル=1, EOBとなる。これを輝度信号とし、例えばMPEG2方式の可変長符号化表により符号化する。MPEG2方式の可変長符号化表を、直流成分に関して図6、交流成分に関して図7に示す。

【0035】図6において、送信符号は「符号語」71と「付加ビット」72を連続させたものとする。

【0036】また図7において、「R/L」81は0ラン/レベルの組み合わせを示し、「長」82は符号語のビット長を示す。送信符号は「符号語」83で示すデータである。また、「escape」84はこの表で表現できない組み合わせに対する送信データで、85に詳細を示してある。ここで、「R」86が0ラン、「L」87がレベル。88と89を連続した並べたものが送信データとなる。なお、図7には、『注1)最後のビット“s”が“0”のとき+を、“1”のとき-を表す。注2)最初の係数で使われるこのコードはEOBと重なっている。注3)2回目以降で使われるコードである。』のような注意がある。なお、図6、図7は、「ISO/IEC 13818」を転記したものである。

【0037】さて、これらの図を使うと、符号化結果は順に、

1101 111, 0100 1,  
0011 11, 0000 0010 111,  
0000 1000, 0110, 10  
となる。

【0038】次に、低周波成分はスクランブルを掛けず、高周波成分のみスクランブルを掛ける。例として、前記データにおいて、DC、およびラン/レベルを1ペアのまま送信し、その後スクランブルを掛けるものとする。即ちまず、

1101 111, 0100 1

をそのまま送信する。次にスクランブルを掛けるわけだが、このとき鍵を使った生成多項式により発生したランダムデータを5ビットずつ区切り、結果として0~31

のランダムデータを発生するようにする。生成多項式により発生したランダムデータを例えば、

00010, 10010, 00110, 00011

とすると、5ビットづつに区切ると2, 18, 6, 3となる。

【0039】最初に、ラン=3/レベル=-1である“001111”に対してスクランブルを掛ける。

【0040】“0011 11”は6ビットである。ビット長が6ビットとなる出力はこれも合わせ、全部で“0010 10”(ラン=0/レベル=3)、“001011”(ラン=0/レベル=-3)、“001110”(ラン=3/レベル=1)、“0011 11”(ラン=3/レベル=-1)、“0011 00”(ラン=4/レベル=1)、“001101”(ラン=4/レベル=-1)なる6パターンである。なお、下線が引いてあるパターンがラン=3/レベル=-1のパターンを示す。

【0041】スクランブル用のランダムデータが最初は2であるから、前記パターンをMPEG2方式の可変長符号化表の図7の順に並べ、“0011 11”から2番目のデータ、即ち“0011 01”を抽出し、送信する。

【0042】次に、ラン=2/レベル=-3である“0000 0010 111”に対してスクランブルを掛ける。

【0043】これは11ビットである。ビット長が11ビットとなる出力はこれも合わせ、全部で、“0000 0010 100”、“0000 0010 101”、“0000 0011 000”、“0000 0011 001”、“0000 0010 110”、“0000 0010 111”、“0000 0011 110”、“0000 0011 111”、“0000 0010 010”、“0000 0010 011”、“0000 0011 100”、“0000 0011 101”、“0000 0011 010”、“0000 0011 011”、“0000 0010 000”、“0000 0010 001”なる16パターンである。

【0044】そこで、スクランブル用のランダムデータが2番目は18であるから、前記パターンをMPEG2方式の可変長符号化表の図7の順に並べ、“0000 0010 111”から18番目のデータ、即ち“0000 0011 111”を抽出し、送信する。なお、最後(“0000 0010 001”)まで行ったら、最初(“0000 0010 100”)に折り返す。

【0045】次に、ラン=2/レベル=2である“0000 1000”に対してスクランブルを掛ける。

【0046】スクランブル用のランダムデータの3番目は6であるから、前記と同様にMPEG2方式の可変長

符号化表の図7の順に並べ、“0000 1000”から6番目のデータである“0000 1100”を送信する。

【0047】次に、ラン=1/レベル=1である“0110”に対してスクランブルを掛ける。

【0048】スクランブル用のランダムデータが4番目は3であるから、前記と同様にMPEG2方式の可変長符号化表の図7の順に並べ、“0110”から3番目のデータである“0111”を送信する。

【0049】そして最後にEOB（エンドオブブロック、“10”）を送信する。即ち、  
0011 01, 0000 0011 111, 0000 1100, 0111, 10

を送信する。全送信データをまとめると、

1101 111, 0100 1,  
0011 01, 0000 0011 111,  
0000 1100, 0111, 10

となる。これがVLC+スクランブル回路出力データ39である。

【0050】次に、受信側における動作について説明する。

【0051】デスクランブル+VLD回路入力データ41はVLC+スクランブル回路出力データ39と同じである。

【0052】受信契約者に関しては、鍵が分かっているため、送信側と逆の動作を行い、デスクランブル+VLD回路出力データ49で、

1101 111, 0100 1,  
0011 11, 0000 0010 111,  
0000 1000, 0110, 10

なるデータを得ることができ、そこから、DC=15, ラン=0/レベル=-2, ラン=3/レベル=-1, ラン=2/レベル=-3, ラン=2/レベル=2, ラン=1/レベル=1, EOBと、図4のデータが完全に復元できる。

【0053】しかしながら、受信契約をしていない人に対しては、鍵が分かっておらず、

1101 111, 0100 1,  
0011 01, 0000 0011 111,  
0000 1100, 0111, 10

なるデスクランブル+VLD回路入力データ41をそのままデコードすることになる。即ち、前記可変長データを図6、図7に従って可変長復号化すると、デスクランブル+VLD回路出力データ49は、DC=15, ラン=0/レベル=-2, ラン=4/レベル=-1, ラン=4/レベル=-2, ラン=0/レベル=4, ラン=1/レベル=-1, EOBとなり、図5のデータが得られる。そして、このデータを逆量子化、2次元DCT変換を行なうことになる。これは、低周波成分は正しいデータだが高周波成分は誤ったデータとなっているため、映

像信号になったとき映像の大まかな概要は分かるが、細かい内容が分からないという特徴を持つ。

【0054】次に、他の実施例について説明する。

【0055】図8に本発明の第2の実施例による映像送信装置および映像受信装置を示す。図17に示す映像送信装置および映像受信装置との相違点は、スクランブル回路117がコーデック（圧縮）ブロック11の後ではなくその前に設けられ、また、デスクランブル回路124がコーデック（伸長）ブロック12の前ではなくその後に設けられていることである。スクランブル回路117は、MPEG2方式により圧縮した映像信号に対し、グループオブピクチャー内でピクチャーデータをスクランブルに従った特定の順序で並べ変える。デスクランブル回路124は、スクランブル回路117によって並べ変えた順序を元の順序に戻す。

【0056】グループオブピクチャー内のピクチャー数が15であるとする。このとき、スクランブル出力を4ビットずつ区切ってピクチャーの順序とする。4ビットずつ区切ったスクランブル出力が、例えば、3, 11, 8, 15, 0, 14, 8, 2, …と続いたとする。このとき、送信ピクチャー順は、3, 11, 8と続く。ただし、グループオブピクチャー内のピクチャー数が15のとき0~14が有効のため、4番目の「15」はスキップされ、また全ピクチャーができる前の2回目の出現である7番目の「8」もスキップされる。

【0057】スクランブルの順に送り続けてもいいし、スクランブル出力が1巡した順序を記憶しておき、その後ずっとその順序を使っても良い。

【0058】これにより、受信側でスクランブルデコーダ（デスクランブル回路124）を用いてデコードすれば、オリジナルの順で映像が再生でき、スクランブルデコーダなしでデコードすれば、フレーム順の入れ替わった映像が再生され、見にくい映像が再現される。

【0059】図9に本発明の第3の実施例による映像送信装置および映像受信装置を示す。図17に示す映像送信装置および映像受信装置との相違点は、スクランブル回路117Aがコーデック（圧縮）ブロック11の後ではなくコーデック（圧縮）ブロック11A内のスキャン変換回路112の後に設けられ、また、デスクランブル回路124Aがコーデック（伸長）ブロック12の前ではなくコーデック（伸長）ブロック12A内のスキャン逆変換回路128の前に設けられていることである。スクランブル回路117Aは、MPEG2方式により圧縮した映像信号に対し、ピクチャー内でスライスデータをスクランブルに従った特定の順序で並べ変える。デスクランブル回路124Aは、スクランブル回路117Aによって並べ変えた順序を元の順序に戻す。

【0060】ピクチャー内のスライス数が30であるとする。このとき、スクランブル出力を5ビットずつ区切ってピクチャーの順序とする。4ビットずつ区切ったス

クラランブル出力が、例えば、16, 5, 31, 21, 12, 27, 7, 16, ...と続いたとする。このとき、送信ピクチャー順は、16, 5と続く。ただし、ピクチャー内のスライス数が30のとき0~29が有効のため、3番目の「31」はスキップされ、また全てピクチャーができる前の2回目の出現である8番目の「16」もスキップされる。

【0061】スクランブルの順に送り続けてもいいし、スクランブル出力が1巡した順序を記憶しておき、その後ずっとその順序を使っても良い。

【0062】これにより、受信側でスクランブルデコーダ（デスクランブル回路124A）を用いてデコードすれば、オリジナルの順で映像が再生でき、スクランブルデコーダなしでデコードすれば、スライス順の入れ替わった映像が再生され、見にくい映像が再現される。

【0063】図10を参照すると、本発明の第4の実施例による映像送信装置および映像受信装置は、スクランブル回路のスクランブル方式およびデスクランブル回路のデスクランブル方式が相違している点を除いて、図9に示したものと同様の構成を有する。したがって、スクランブル回路およびデスクランブル回路にそれぞれ117Bおよび124Bの参照符号を付してある。スクランブル回路117Bは、MPEG2方式により圧縮した映像信号に対し、スライス内でマクロブロックデータをスクランブルに従った特定の順序で並べ変える。デスクランブル回路124Bは、スクランブル回路117Bによって並べ変えた順序を元の順序に戻す。

【0064】スライス内のマクロブロック数が45であるとする。このとき、スクランブル出力を6ビットづつ区切ってピクチャーの順序とする。6ビットづつ区切ったスクランブル出力が、例えば、42, 34, 18, 6, 59, 24, 37, 51, 29, 32, 11, 42, ...と続いたとする。このとき、送信ピクチャー順は、42, 34, 18と続く。ただし、スライス内のマクロブロック数が45のとき0~44が有効のため、5番目の「59」はスキップされ、また全てピクチャーができる前の2回目の出現である12番目の「42」もスキップされる。

【0065】スクランブルの順に送り続けてもいいし、スクランブル出力が1巡した順序を記憶しておき、その後ずっとその順序を使っても良い。

【0066】これにより、受信側でスクランブルデコーダ（デスクランブル回路124B）を用いてデコードすれば、オリジナルの順で映像が再生でき、スクランブルデコーダなしでデコードすれば、マクロブロック順の入れ替わった映像が再生され、見にくい映像が再現される。

【0067】また、グループオブピクチャー内でのピクチャーのスクランブル、ピクチャー内でのスライスのスクランブル、スライス内でのマクロブロックデータのス

クラランブルに関して、2通り以上の組み合わせを行なっても良い。

【0068】図11にグループオブピクチャー内でのピクチャーのスクランブルとピクチャー内でのスライスのスクランブルとを組み合わせた例を示す。すなわち、この例では、スキャン変換回路112の前後にそれぞれスクランブル回路117および117Aを配置し、スキャン逆変換回路128の前後にそれぞれデスクランブル回路124Aおよび124を配置している。

【0069】また、図12に、ピクチャー内でのスライスのスクランブルとスライス内でのマクロブロックデータのスクランブルとを組み合わせる例を示す。スクランブル回路およびデスクランブル回路にそれぞれ117Cおよび124Cの参照符号を付してある。

【0070】前述したのと同様に、ピクチャー内のスライス数が30、スライス内のマクロブロック数が45であるとする。このとき、スクランブル出力から1回5ビットを取り出してスライス番号とし、その後45回6ビット取り出して前記スライスにおけるマクロブロック番号とし、それを30回続ける。または、11ビット（スライス番号5ビット+マクロブロック番号6ビット）を取り出し、1350（30×45）回繰り返しても良い。また、ピクチャー内のマクロブロック数1350に通し番号を付け、11ビット取り出しを1350回繰り返しても良い。

【0071】他の組み合わせに関しても同様である。なお、上述したように、原映像信号に対して所定の塊内で所定のブロック単位を特定の順序に並べ変えることにより軟らかいスクランブルを掛けることを、原映像信号を「シャフルする」とも呼ぶ。

【0072】さらに、実施例前半で示した可変長符号化表の選択により軟らかいスクランブルを掛ける方法と、実施例後半で示したブロック順を変えることにより軟らかいスクランブルを掛ける（シャフルする）方法とを組み合わせても良い。

【0073】図13に第1の実施例（図1）と第2の実施例（図8）とを組み合わせた例を示す。図14に第1の実施例（図1）と第3の実施例（図9）とを組み合わせた例を示す。図15に第1の実施例（図1）と第4の実施例（図10）とを組み合わせた例を示す。図16に第1の実施例（図1）と第2の実施例（図8）と第3の実施例（図9）とを組み合わせた例を示す。

【0074】なお、低域成分と高域成分の分割位置は任意に選ぶことができる。例えば、低域成分を直流成分のみで高域成分をそれ以外としても良いし、全部の成分を高域成分としても良い。低域成分を、低周波側から規定された個数のラン／レベルの組み合わせとしても良いし、高周波側から規定された個数のラン／レベルの組み合わせ以外の組み合わせとしても良い。

【0075】直交変換はDCT変換以外でも良い。ま



た、DCT変換において、ここでは1ブロックを4画素×4ラインとしているが、8画素×8ライン、16画素×8ライン、16画素×16ライン等、任意に選ぶことができる。

【0076】VLCコード表は実施例に示した以外のものを使っても良い。

【0077】圧縮はMPEG方式に限らないが、直交変換+量子化+可変長符号方式であることが好ましい。例えば、JPEG (Joint Photographic coding Experts Group) 等にも適用できる。

【0078】スクランブル回路は1マクロブロック単位でプリセットしても良いし、1スライス単位、1ピクチャー単位、1グループオブピクチャー単位でプリセットしても良い。スクランブルにおけるランダムデータ発生回路の生成多項式は任意の式で良いし、生成多項式を使わないスクランブル回路にも対応可能である。

【0079】本発明は上述した実施形態に限定せず、本発明の趣旨を逸脱しない範囲内で種々の変更・変形が可能である。

#### 【0080】

【発明の効果】以上説明したように本発明は、原映像信号を圧縮した後及び／又は前に軟らかいスクランブルを掛けることにより送信している。これにより、受信側で受信契約者がスクランブルデコーダ（デスクランブル回路）を用いてデコードすれば、全域データ、即ち完全な映像／音声などのデータを再生することができるが、受信契約をしていない人たちがスクランブルデコーダなしでデコードすれば多少の絵柄が判別できる程度の映像が再生できる。したがって、受信契約をしていない人たちの完全な映像／音声などを見たいという欲求を高め、受信契約の数を増加させることができる、という効果を奏する。

#### 【図面の簡単な説明】

【図1】本発明の一実施の形態（第1の実施例）による映像送信装置と映像受信装置の構成を示すブロック図である。

【図2】図1に示した映像送信装置に使用されるVLC+スクランブル回路を示すブロック図である。

【図3】図1に示した映像受信装置に使用されるデスクランブル+VLD回路を示すブロック図である。

【図4】映像送信装置で2次元DCT変換を行い、さらに量子化を行ったときの行列データを示す図である。

【図5】映像受信装置にデスクランブル回路が存在しないときの逆量子化前の行列データを示す図である。

【図6】MPEG-2方式の可変長符号化表（直流成分）を示す図である。

【図7】MPEG-2方式の可変長符号化表（交流成分）を示す図である。

【図8】本発明の第2の実施例による映像送信装置と映像受信装置の構成を示すブロック図である。

【図9】本発明の第3の実施例による映像送信装置と映像受信装置の構成を示すブロック図である。

【図10】本発明の第4の実施例による映像送信装置と映像受信装置の構成を示すブロック図である。

【図11】本発明の第2の実施例（図8）と第3の実施例（図9）とを組み合わせた映像送信装置と映像受信装置の構成を示すブロック図である。

【図12】本発明の第3の実施例（図9）と第4の実施例（図10）とを組み合わせた映像送信装置と映像受信装置の構成を示すブロック図である。

【図13】本発明の第1の実施例（図1）と第2の実施例（図8）とを組み合わせた映像送信装置と映像受信装置の構成を示すブロック図である。

【図14】本発明の第1の実施例（図1）と第3の実施例（図9）とを組み合わせた映像送信装置と映像受信装置の構成を示すブロック図である。

【図15】本発明の第1の実施例（図1）と第4の実施例（図10）とを組み合わせた映像送信装置と映像受信装置の構成を示すブロック図である。

【図16】本発明の第1の実施例（図1）と第2の実施例（図8）と第3の実施例（図9）とを組み合わせた映像送信装置と映像受信装置の構成を示すブロック図である。

【図17】従来の映像送信装置と映像受信装置の構成を示すブロック図である。

#### 【符号の説明】

11, 11A, 11B, 11C	コーデック（圧縮）ブロック
111	原画像（原映像信号）
112	スキャン変換回路
113	DCT変換回路
114	量子化回路
115	符号量制御回路
116	可変長符号化（VLC）回路
117, 117A, 117B, 117C	スクランブル回路
118	ECC付加回路
119	変調回路
120	送信信号
12, 12A, 12B, 12C	コーデック（伸長）ブロック
121	受信信号
122	復調回路
123	ECC処理回路
124, 124A, 124B, 124C	デスクランブル回路
125	可変長復号（VLD）回路
126	逆量子化回路
127	逆DCT変換回路
128	スキャン逆変換回路

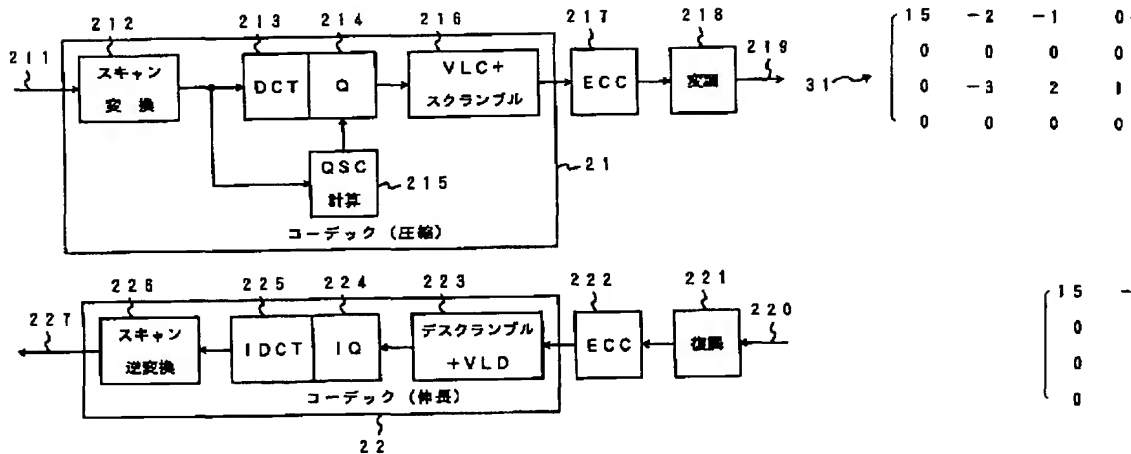


- 1 2 9 再生画像  
 2 1, 2 1 A, 2 1 B コーデック (圧縮) ブロック  
 2 1 1 原画像 (原映像信号)  
 2 1 2 スキャン変換回路  
 2 1 3 DCT変換回路  
 2 1 4 量子化回路  
 2 1 5 符号量制御回路  
 2 1 6 可変長符号化 (VLC) + スランブル回路  
 2 1 7 ECC付加回路  
 2 1 8 変調回路  
 2 1 9 送信信号  
 2 2, 2 2 A, 2 2 B コーデック (伸長) ブロック  
 2 2 0 受信信号  
 2 2 1 復調回路  
 2 2 2 ECC処理回路  
 2 2 3 デスクランブル+可変長復号 (VLD) 回路  
 2 2 4 逆量子化回路  
 2 2 5 逆DCT変換回路  
 2 2 6 スキャン逆変換回路

- 2 2 7 再生画像  
 3 1 VLC+スランブル回路入力データ  
 3 2 高域/低域成分分離回路  
 3 3 低域成分  
 3 4 高域成分  
 3 5 タイミング調整用メモリ  
 3 6 VLCシフト回路  
 3 7 スランブル回路  
 3 8 統合回路  
 3 9 VLC+スランブル回路出力データ  
 4 1 デスクランブル+VLD回路入力データ  
 4 2 高域/低域成分分離回路  
 4 3 低域成分  
 4 4 高域成分  
 4 5 タイミング調整用メモリ  
 4 6 VLDシフト回路  
 4 7 デスクランブル回路  
 4 8 高域/低域成分統合回路  
 4 9 デスクランブル/VLD回路出力データ

【図1】

【図4】

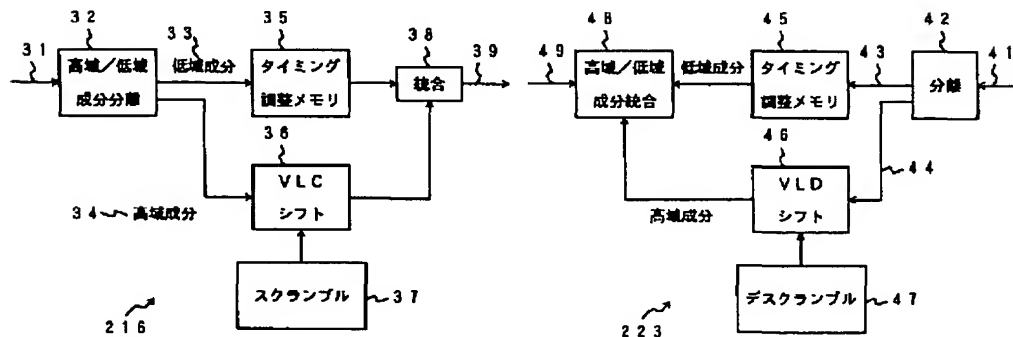


【図5】

$$\begin{bmatrix} 15 & -2 & 0 & 0 \\ 0 & 0 & 0 & 4 \\ 0 & 0 & -2 & 0 \\ 0 & 0 & -1 & 0 \end{bmatrix}$$

【図2】

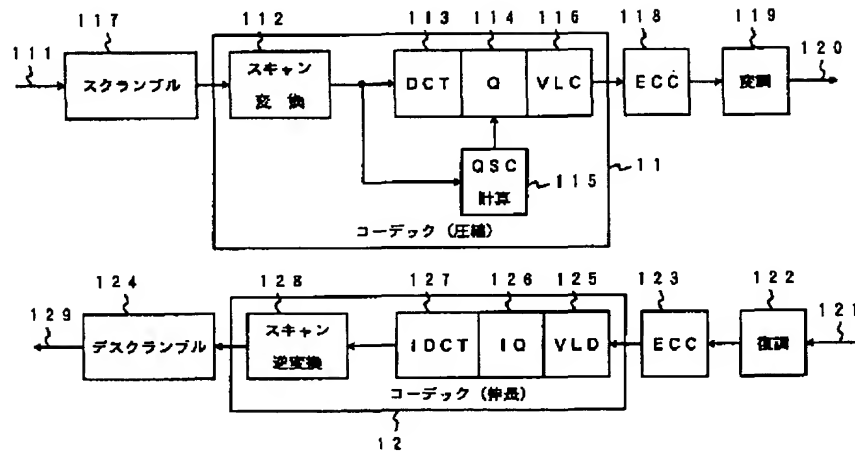
【図3】



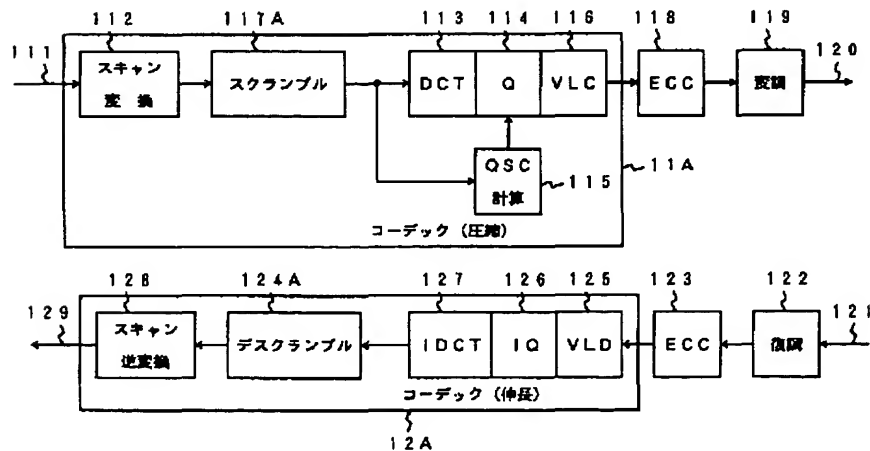
【図6】

差分DC値	全符号長	符号語	付加ビット
-2047~-1024	9+11	1111 1111 1	000000000~0111111111
-1023~-512	9+10	1111 1111 0	000000000~0111111111
-511~-256	8+9	1111 1110	000000000~0111111111
-255~-128	7+8	1111 110	000000000~0111111111
-127~-64	6+7	1111 10	000000000~0111111111
-63~-32	5+6	1111 0	000000000~0111111111
-31~-16	4+5	1110	000000000~0111111111
-15~-8	3+4	110	000000000~0111111111
-7~-4	3+3	101	000~011
-3~-2	2+2	01	00~01
-1	2+1	00	0
0	3	100	-
1	2+1	00	1
2~3	2+2	01	10~11
4~7	3+3	101	100~111
8~15	3+4	110	1000~1111
16~31	4+5	1110	10000~11111
32~63	5+6	1111 0	100000~111111
64~127	6+7	1111 10	1000000~1111111
128~255	7+8	1111 110	10000000~11111111
256~511	8+9	1111 1110	100000000~111111111
512~1023	9+10	1111 1111 0	1000000000~1111111111
1024~2047	9+11	1111 1111 1	10000000000~11111111111

【図8】



【図9】



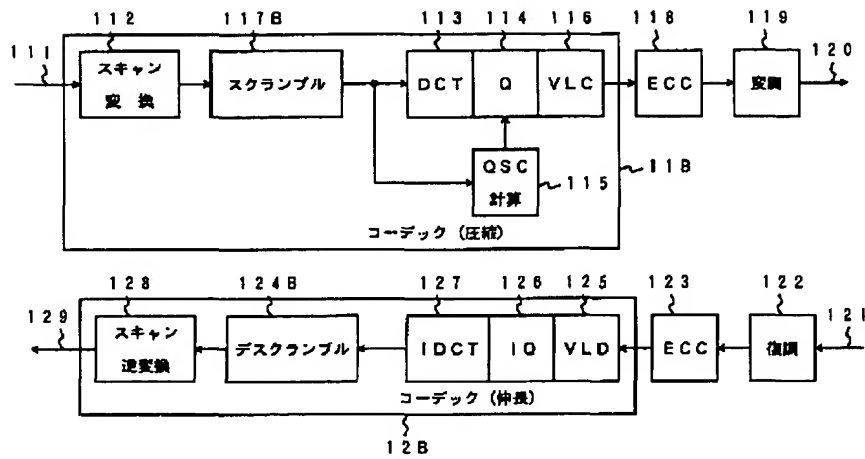
【図7】

81 82 83								
R/L	長	符号語	R/L	長	符号語	R/L	長	符号語
E08	2	10	1/5	13	0000 0001 1011 s	0/26	15	0000 0000 0101 01s
0/1	2	1 s (注2)	2/4	13	0000 0001 0100 s	0/27	15	0000 0001 0101 00s
0/1	3	11 s (注3)	3/3	13	0000 0001 1100 s	0/28	15	0000 0001 0100 11s
1/1	4	011 s	4/3	13	0000 0001 0010 s	0/29	15	0000 0001 0100 10s
0/2	5	0100 s	6/2	13	0000 0001 1110 s	0/30	15	0000 0001 0100 01s
2/1	5	0101 s	7/2	13	0000 0001 0101 s	0/31	15	0000 0001 0100 00s
0/3	6	0010 1 s	8/2	13	0000 0001 0001 s	0/32	16	0000 0001 0011 000s
3/1	6	0011 1 s	17/1	13	0000 0001 1111 s	0/33	16	0000 0001 0010 111s
4/1	6	0011 0 s	18/1	13	0000 0001 1010 s	0/34	16	0000 0001 0010 110s
1/2	7	0001 10 s	19/1	13	0000 0001 1001 s	0/35	16	0000 0001 0010 101s
5/1	7	0001 11 s	20/1	13	0000 0001 0111 s	0/36	16	0000 0001 0010 100s
6/1	7	0001 01 s	21/1	13	0000 0001 0110 s	0/37	16	0000 0001 0010 011s
7/1	7	0001 00 s	0/12	14	0000 0000 1101 0 s	0/38	16	0000 0000 0010 010s
0/4	8	0000 110 s	0/13	14	0000 0000 1100 1 s	0/39	16	0000 0000 0010 001s
2/2	8	0000 100 s	0/14	14	0000 0000 1100 0 s	0/40	16	0000 0000 0010 000s
8/1	8	0000 111 s	0/15	14	0000 0000 1011 1 s	1/8	16	0000 0000 0011 111s
9/1	8	0000 101 s	1/6	14	0000 0000 1011 0 s	1/9	16	0000 0000 0011 110s
84 ~ escape	6	0000 01	1/7	14	0000 0000 1010 1 s	1/10	16	0000 0000 0011 101s
0/5	9	0010 0110 s	2/5	14	0000 0000 1010 0 s	1/11	16	0000 0000 0011 100s
0/6	9	0010 0001 s	3/4	14	0000 0000 1001 1 s	1/12	16	0000 0000 0011 011s
1/3	9	0010 0101 s	5/3	14	0000 0000 1001 0 s	1/13	16	0000 0000 0011 010s
3/2	9	0010 0100 s	9/2	14	0000 0000 1000 1 s	1/14	16	0000 0000 0011 001s
10/1	9	0010 0111 s	10/2	14	0000 0000 1000 0 s	1/15	17	0000 0000 0001 0011s
11/1	9	0010 0011 s	22/1	14	0000 0000 1111 1 s	1/16	17	0000 0000 0001 0010s
12/1	9	0010 0010 s	23/1	14	0000 0000 1111 0 s	1/17	17	0000 0000 0001 0001s
13/1	9	0010 0000 s	24/1	14	0000 0000 1110 1 s	1/18	17	0000 0000 0001 0000s
0/7	11	0000 0010 10 s	25/1	14	0000 0000 1110 0 s	6/3	17	0000 0000 0001 0100s
1/4	11	0000 0011 00 s	26/1	14	0000 0000 1101 1 s	11/2	17	0000 0000 0001 1010s
2/3	11	0000 0010 11 s	0/16	15	0000 0000 0111 11 s	12/2	17	0000 0000 0001 1001s
4/2	11	0000 0011 11 s	0/17	15	0000 0000 0111 10 s	13/2	17	0000 0000 0001 1000s
5/2	11	0000 0010 01 s	0/18	15	0000 0000 0111 01 s	14/2	17	0000 0000 0001 0111s
14/1	11	0000 0011 10 s	0/19	15	0000 0000 0111 00 s	15/2	17	0000 0000 0001 0110s
15/1	11	0000 0011 01 s	0/20	15	0000 0000 0110 11 s	16/2	17	0000 0000 0001 0101s
16/1	11	0000 0010 00 s	0/21	15	0000 0000 0110 10 s	27/1	17	0000 0000 0001 1111s
0/8	13	0000 0001 1101 s	0/22	15	0000 0000 0110 01 s	28/1	17	0000 0000 0001 1110s
0/9	13	0000 0001 1000 s	0/23	15	0000 0000 0110 00 s	29/1	17	0000 0000 0001 1101s
0/10	13	0000 0001 0011 s	0/24	15	0000 0000 0101 11 s	30/1	17	0000 0000 0001 1100s
0/11	13	0000 0001 0000 s	0/25	15	0000 0000 0101 10 s	31/1	17	0000 0000 0001 1011s

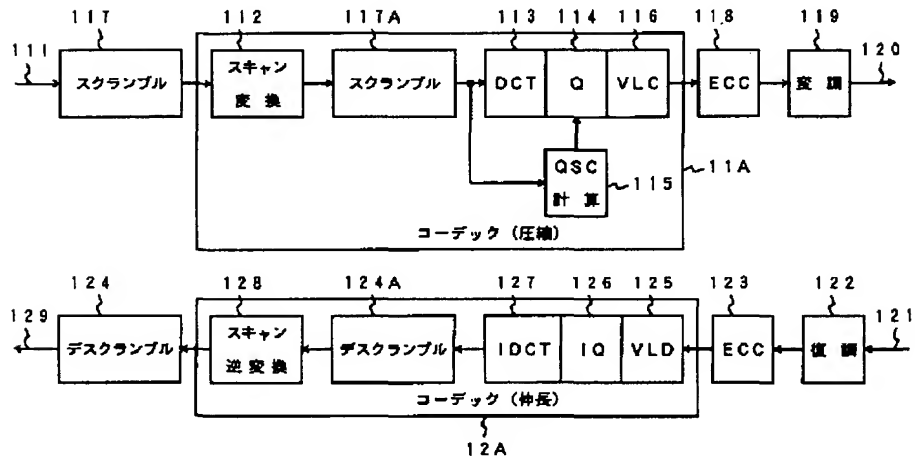
  

86 88		85 87 89	
R(Run)	escape(Fixed Length Code)	L (Level)	escape(Fixed Length Code)
0	0 0 0 0 0 0	-2 0 4 7	1 0 0 0 0 0 0 0 1
1	0 0 0 0 0 1	-2 0 4 6	1 0 0 0 0 0 0 0 0
2	0 0 0 0 1 0	.	.
3	0 0 0 0 1 1	.	.
4	0 0 0 1 0 0	.	.
.	.	-2	.
.	.	-1	1 1 1 1 1 1 1 1 0
.	.	禁止	1 1 1 1 1 1 1 1 1
.	.	1	0 0 0 0 0 0 0 0 0
.	.	2	0 0 0 0 0 0 0 0 1
.	.	.	0 0 0 0 0 0 0 0 0
5 9	1 1 1 1 0 1 1	.	.
6 0	1 1 1 1 1 0 0	.	.
6 1	1 1 1 1 1 0 1	2 0 4 6	0 1 1 1 1 1 1 1 0
6 2	1 1 1 1 1 1 0	2 0 4 7	0 1 1 1 1 1 1 1 1
6 3	1 1 1 1 1 1 1		

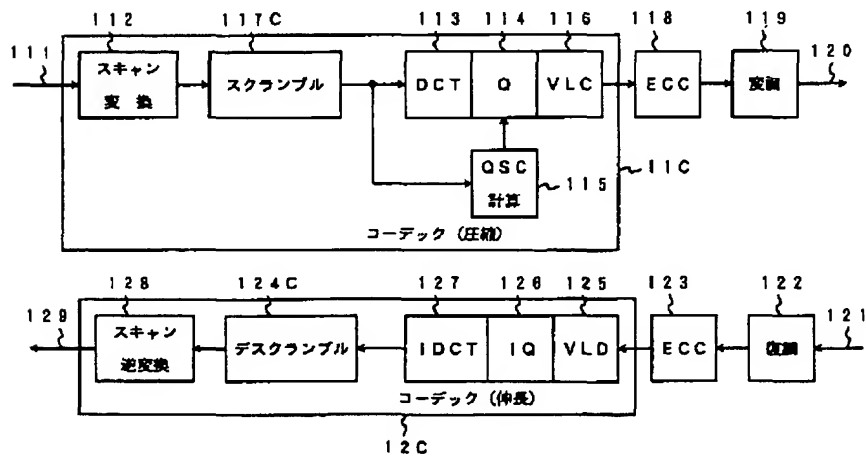
【図10】



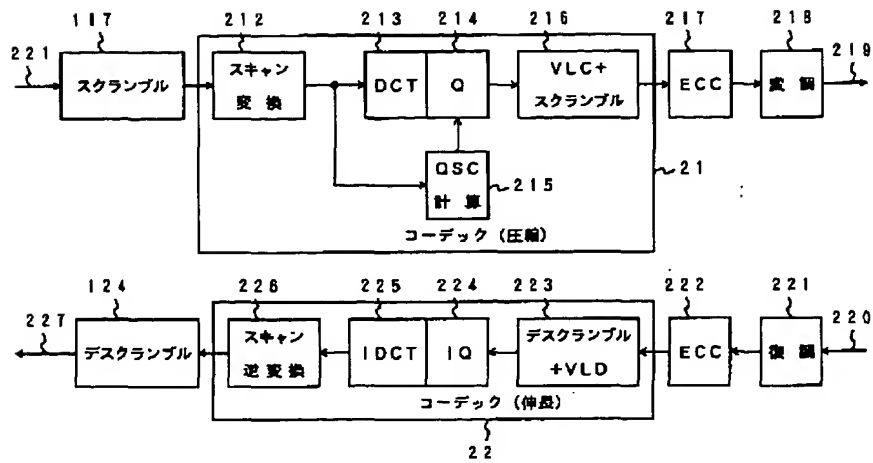
【図11】



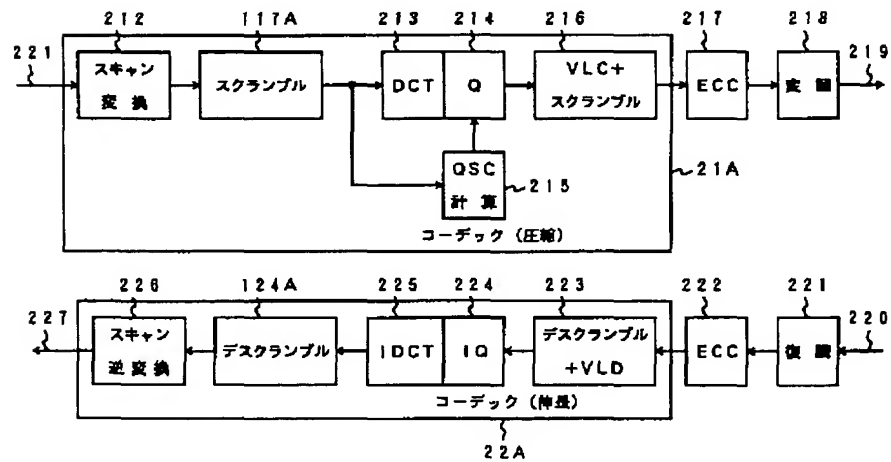
【図12】



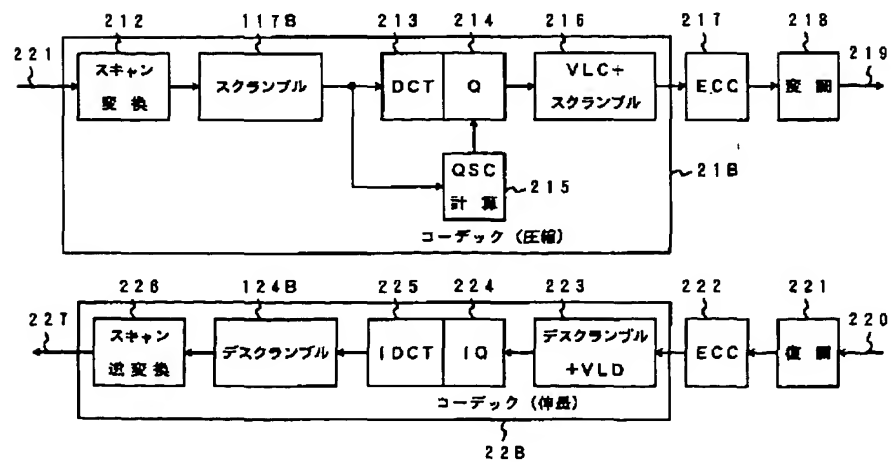
【図13】



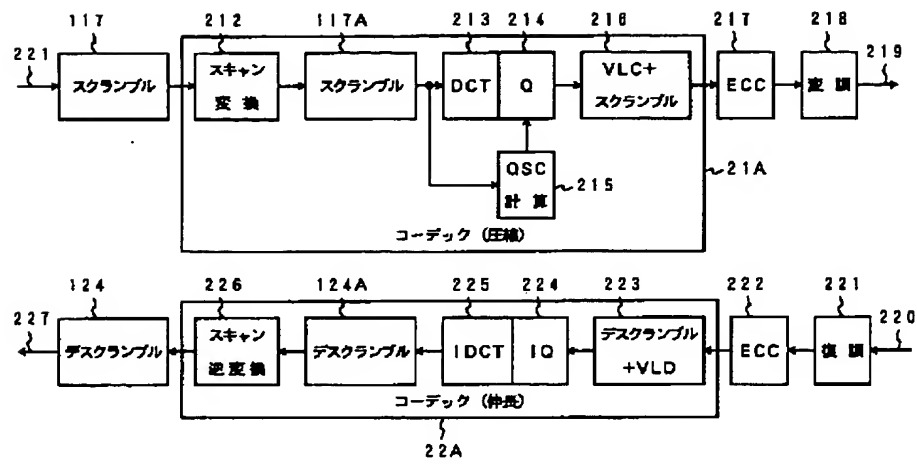
【図14】



【図15】



【図16】



【図17】

